Democratic and effective oversight of national security services

Issue paper

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Democratic and effective oversight of national security services

Issue paper published
by the Council of Europe
Commissioner for Human Rights

Council of Europe

Issue papers are published by the Commissioner for Human Rights to contribute to debate and reflection on important current human rights issues. Many of them also include recommendations by the Commissioner for addressing the concerns identified. The opinions expressed in these expert papers do not necessarily reflect the Commissioner's position.

Issue papers are available on the Commissioner's website: www.commissioner.coe.int

Cover photos: © Shutterstock
Cover: Documents and Publications Production Department (SPDP), Council of Europe
Layout: Jouve, Paris

Printed at the Council of Europe

Acknowledgements:

This issue paper was prepared by Mr Aidan Wills, independent consultant.

Contents

EXECUTIVE SUMMARY

Ongoing revelations by former US intelligence contractor Edward Snowden have brought renewed attention to the activities of security services in Council of Europe member states. Concerns about the implications of large-scale electronic surveillance activities have once again given rise to questions about the adequacy of the oversight of security services. The oversight of security services is fundamental to ensuring that these institutions both contribute to the protection of the populations they serve and respect the rule of law and human rights in undertaking this task. However, the Snowden revelations, the involvement of some European security services in the secret detention and extraordinary rendition of terrorist suspects and allegations about unlawful security service activity in various Council of Europe member states have cast significant doubt on the capacity of national oversight systems to perform this role.

Against this background, this issue paper addresses the question of what is required to make national oversight systems more effective in helping to promote human rights compliance and accountability in the work of security services.

This issue paper focuses on the oversight of state bodies, including both autonomous agencies and departments/units of other government departments or the armed forces, that have a mandate to collect, analyse and disseminate intelligence within the borders of their state in order to inform decisions by policy makers, military commanders, police investigators and border/customs agencies about threats to national security and other core national interests. Although some security services do exercise powers of arrest and detention, the oversight of such powers is not covered in any detail in this issue paper.

The Council of Europe Commissioner for Human Rights has formulated a number of recommendations on the basis of the issues raised by this issue paper; these are set out after this executive summary.

1. OVERVIEW OF THE IMPACT OF NATIONAL SECURITY SERVICES' ACTIVITIES ON HUMAN RIGHTS PROTECTION IN EUROPE

Contemporary examples of the impact that security service activities have on human rights are discussed in connection with four areas.

First, there are activities that impact upon personal integrity including the right to life, the right to personal liberty and security, and the right not to be subjected to torture or inhuman, cruel and degrading treatment. Examples given include involvement in the rendition and secret detention of terrorist suspects; information sharing leading to rendition, torture and drone strikes; and ongoing arrests and arbitrary detention by security services.

Second, security service activities impact upon the right to privacy and family life. In most jurisdictions this is the most common way in which security services interfere with human rights. Bulk surveillance and the exploitation of communications data/metadata are considered in some detail, and consideration is also given to the privacy implications of computer network exploitation and international intelligence sharing.

Third, security service activity has implications for the rights to freedom of expression, association and assembly. Both direct and indirect interferences with these rights are discussed, including the chilling effect on these rights created by potential and actual use of surveillance measures. Also discussed is the broader harm done to democratic processes by security service interference with politicians, judges and non-governmental organisations (NGOs).

Finally, brief consideration is given to the impact on the right to a fair trial, including the implications of security service surveillance of lawyer–client communications and the threat to a fair trial posed by measures adopted to protect state secrets in litigation relating to security services.

2. OVERVIEW OF INTERNATIONAL AND EUROPEAN STANDARDS CONCERNING DEMOCRATIC OVERSIGHT OVER NATIONAL SECURITY SERVICES

International and European standards on the oversight of security services are divided into binding legal instruments and non-binding principles or recommendations. The first category includes provisions from a number of international and regional treaties, as well as their interpretations by relevant courts or treaty bodies. Although there are very few international or regional legal instruments that are directly applicable to oversight, it has been shown that a number of requirements that are of direct relevance to security service oversight can be derived from the European Court of Human Rights' ("the Court" or "the Strasbourg Court") jurisprudence on Articles 3, 5, 8 and 13 of the European Convention on Human Rights ("the Convention" or "ECHR") in particular. These include requirements for: the effective investigation of serious human rights violations; effective remedies in relation to human rights violations by security services, including in the context of secret surveillance; *ex ante* authorisation of intrusive surveillance measures; and *ex post* review of surveillance measures.

The second category includes recommendations, resolutions, declarations and reports from four sources: (i) United Nations (UN) institutions, including the General Assembly and special mandate holders; (ii) Council of Europe institutions, including the Venice Commission, the Parliamentary Assembly (PACE) and its rapporteurs and the Commissioner for Human Rights; (iii) the European Union; and (iv) civil society-led transnational initiatives. There has been a proliferation of such documents in the past 10 years to the extent that there is now a comprehensive lexicon of soft-law principles on oversight; the key or novel recommendations from each are presented and any significant differences highlighted.

The most comprehensive sets of principles are the UN compilation of good practices on intelligence agencies and their oversight (UN 2010a) – put forward by the former UN Special Rapporteur on human rights and counter-terrorism – and the landmark report of the Venice Commission on the democratic oversight of security services. A number of other reports and resolutions have dealt with the oversight of security services as part of broader assessments. Especially significant are the recommendations put forward in light of the Snowden revelations by the UN special mandate holders, the Council of Europe Commissioner for Human Rights, the PACE and the European Parliament.

The Global Principles on National Security and the Right to Information (the Tshwane Principles) are dealt with in some detail as they provide comprehensive guidance on the key issues of access to information by oversight bodies and public access to documents held by security services and their oversight bodies. Other principles discussed include the Ottawa Principles and the so-called Necessary and Proportionate Principles.

3. NATIONAL PRACTICES IN COUNCIL OF EUROPE MEMBER STATES

Council of Europe member states have taken diverse approaches to structuring and undertaking oversight of their security services. This chapter (Chapter 4) considers national approaches to oversight by: parliamentary committees; independent oversight institutions including expert security/intelligence oversight bodies and institutions with broader jurisdictions such as ombudspersons and data/information commissioners; and judicial bodies, including quasi-judicial bodies. The roles of political executives, security services' internal control mechanisms and informal oversight by civil society and the media are examined briefly. Rather than examining entire national oversight systems, examples are drawn from parts of various countries' systems. This is done with a view to highlighting contrasting approaches and good practices.

It is emphasised that there is no Council of Europe member state whose system of oversight comports with all of the internationally or regionally recognised principles and good practices discussed in this issue paper and that there is no one best approach to organising a system of security service oversight. Nevertheless, this issue paper seeks to highlight particular approaches or practices that offer significant advantages from the point of view of human rights protection.

Parliamentary committees

Detailed consideration is given to the mandates and role of parliamentary oversight committees, which have traditionally been regarded as the principal bodies responsible for oversight of security services. Access to classified information by parliamentary oversight committees is an essential feature of effective oversight; this is addressed alongside the vexed issue of security vetting for parliamentarians and alternative measures for the protection of information. This section (4.1) also addresses the often-overlooked issue of the relationship between parliamentary committees and other oversight bodies.

Independent oversight institutions

Expert security/intelligence oversight institutions play an increasingly prominent role in the supervision of security services. This issue paper adopts the view that they are fundamental to enhancing the efficacy of oversight and improving human rights protection.

Expert security/intelligence oversight bodies have become increasingly common in the Council of Europe area and are often best placed to conduct detailed day-to-day oversight of the legality of security service activity. While emphasising the advantages of these bodies, consideration is given to the steps that can be taken to ensure such bodies are endowed with a level of democratic legitimacy.

Data protection authorities and ombudspersons play a limited role in the oversight of security services in most Council of Europe member states. However, examples are given of the ways in which these bodies can contribute to a system of effective oversight.

Judicial bodies

Judicial bodies are primarily discussed with reference to the authorisation of intrusive surveillance measures. Attention is drawn to the fact that very few states require judicial authorisation for bulk surveillance measures, access to communications data or the use of computer network exploitation. This area of law lags behind developments in surveillance measures and, consequently, measures that are at least as intrusive as traditional security service methods are not subject to judicial authorisation in most jurisdictions. This situation is changing and examples are given of Council of Europe member states that are now requiring judicial checks for untargeted surveillance and for accessing/mining communications data that have been collected. The practice of including special or public interest advocates in authorisation processes to represent the interests of would-be targets is cited with approval.

Quasi-judicial authorisation bodies

Several Council of Europe member states have established quasi-judicial bodies to authorise intrusive methods. The new Belgian system is presented in some detail and reference is made to the fact that Belgium is one of the very few countries whose law requires that computer network exploitation be subject to independent authorisation. The advantages of these specialised authorisation bodies are considered, including the fact that, unlike judicial bodies, they can be accountable to another oversight body.

Internal controls

Although the internal controls within security services are not a focus of this issue paper, it is essential to note that it is individual members of security services that play the most significant role in ensuring that security service activity is human rights compliant and accountable. External oversight can achieve little if the security services do not have an internal culture and members of staff that respect human rights.

4. TOWARDS A DEMOCRATIC AND EFFECTIVE OVERSIGHT OF NATIONAL SECURITY SERVICES

Drawing upon international standards and national practices, this chapter (Chapter 5) sets out the most significant objectives and overriding principles that can enable more effective oversight of security services. A number of headline points are mentioned for the purposes of this summary.

Keeping oversight democratic

Democratic oversight is important because security services (and related executive departments) provide a public service to and on behalf of the public and therefore elected representatives should be involved in ensuring that this service is provided effectively, efficiently and lawfully. The "democratic" aspect of oversight is primarily achieved through the involvement of parliament, including by: ensuring that national laws provide for comprehensive oversight of security services; allocating the necessary budgetary resources to non-parliamentary oversight institutions; overseeing the work of expert oversight bodies; keeping under review the efficacy of oversight institutions; and conducting both ongoing scrutiny and ad hoc inquiries into security service activity.

Ex ante authorisation of intrusive powers

Independent *ex ante* authorisation should be extended to: untargeted bulk collection of information; the collection of and access to communications data (including when held by the private sector); and, potentially, computer network exploitation. The process by which intrusive measures are authorised or re-authorised should itself be subject to scrutiny. Given the difficulties that may arise when seeking to evaluate judicial decisions on the authorisation of intrusive measures, consideration may be given to quasi-judicial models.

Complaints handling

Most oversight bodies can only issue recommendations to security services and/or the executive. Given that the European Convention on Human Rights requires that persons who believe (or know) that their rights have been unlawfully infringed by security services must have access to an institution that can provide an effective remedy, states must ensure that individuals can also access an institution equipped to make legally binding orders.

Access to information related to international intelligence co-operation

Access to information arising from and pertaining to international intelligence co-operation merits special consideration. In view of the extensive international co-operation between security services (and the impact that such co-operation can have on human rights), it is essential that overseers are able to scrutinise information

about such co-operation, including information that has been received from or sent to foreign bodies. Making sure that overseers are not regarded as "third parties" or subject to the principle of originator control either in law or in practice is essential for ensuring proper scrutiny of these activities.

Resources for oversight bodies

Most security services have growing capacities (by virtue of technological changes and increased budgets) to collect, share and receive information and use increasingly complex systems for doing so. Accordingly, recourse to independent technical expertise has become indispensable for effective oversight. Intelligence collection and storage systems have become more complex and their human rights implications cannot easily be assessed without recourse to specialist expertise.

Evaluating oversight systems: who is watching the overseers?

While progress has been made in the Council of Europe area on establishing external oversight of security services, very few countries have gone on to undertake reviews of the efficacy of these systems.

In order to be effective in preventing and responding to human rights concerns in or arising from the work of security services, they require an appropriate legal mandate and powers, resources and expertise. Such requirements evolve as the nature of security service work evolves. It is therefore essential that oversight systems are periodically evaluated to assess whether or not they possess the necessary attributes to be effective. Evaluations may be periodic or ad hoc; it may be effective to include an evaluation requirement in legislation governing oversight bodies.

COMMISSIONER'S RECOMMENDATIONS

Taking into account the findings and conclusions of this issue paper, the Commissioner makes the following recommendations aimed at strengthening oversight of national security services and thereby improving human rights compliance in the work of security services.

In order to ensure that the operations, policies and regulations of security services comply with Convention rights and are subject to effective democratic oversight, the Commissioner calls on the member states of the Council of Europe to:

On general parameters for a system of oversight

1. Establish or designate one or more bodies that are fully independent from the executive and the security services to oversee all aspects of security service regulations, policies, operations and administration. All references to oversight bodies in these recommendations are to independent oversight bodies as defined in these recommendations.
2. Ensure that their systems for the oversight of security services comply with the minimum oversight requirements set out in the European Court of Human Rights' jurisprudence, the UN compilation of good practices on intelligence agencies and their oversight (UN 2010a), as well as the recommendations put forward by the Venice Commission.

On the scope of oversight of security services

3. Ensure that all aspects and phases of the collection (regardless of its method of collection or provenance), processing, storage, sharing, minimisation and deletion of personal data by security services are subject to oversight by at least one institution that is external to the security services and the executive.
4. Ensure that the oversight of security services focuses not only on the lawfulness of security service activities that restrict the right to privacy and family life but also the rights to freedom of expression, assembly, association and religion, thought and conscience.

5. 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, joint operations and the provision of equipment and training. External oversight of security service co-operation with foreign bodies should include but not be limited to examining:
    a. ministerial directives and internal regulations relating to international intelligence co-operation;
    b. human rights risk assessment and risk-management processes relating to relationships with specific foreign security services and to specific instances of operational co-operation;
    c. outgoing personal data and any caveats (conditions) attached thereto;
    d. security service requests made to foreign partners: (i) for information on specific persons; and (ii) to place specific persons under surveillance;
    e. intelligence co-operation agreements;
    f. joint surveillance operations and programmes undertaken with foreign partners.
6. Require that security services obtain authorisation from a body that is independent from the security services and the executive, both in law and in practice, before engaging in any of the following activities either directly or through/in collaboration with private sector entities:
    a. conducting untargeted bulk surveillance measures regardless of the methods or technology used or the type of communications targeted;
    b. using selectors or key words to extract data from information collected through bulk surveillance, particularly when these selectors relate to identifiable persons;
    c. collecting communications/metadata directly or accessing it through requests made to third parties, including private companies;
    d. accessing personal data held by other state bodies;
    e. undertaking computer network exploitation.
7. Ensure that, where security services engage in computer network exploitation, these activities are subject to the same level of external oversight as is required for surveillance measures that have equivalent human rights implications.
8. Consider the introduction of security-cleared public interest advocates into surveillance authorisation processes, including both targeted and untargeted surveillance measures, to represent the interests of would-be targets of surveillance.
9. Consider how surveillance authorisation processes can be kept under *ex post facto* review by an independent body that is empowered to examine decisions taken by the authorising body.
10. Create or designate an external oversight body to receive and investigate complaints relating to all aspects of security service activity. Where such bodies are

only empowered to issue non-binding recommendations, member states must ensure that complainants also have recourse to another institution that can provide remedies that are effective both in law and in practice.

11. Give an external oversight body the power to quash surveillance warrants and discontinue surveillance measures undertaken without the need for a warrant when such activities are deemed to have been unlawful, as well as the power to require the deletion of any information obtained from the use of such measures.

12. Ensure that the procedures of any institution tasked with adjudicating on complaints relating to matters that have been revealed to a complainant or otherwise made public comply with due process standards under European human rights law.

On the independence and democratic legitimacy of oversight bodies

13. Consider strengthening the link between expert oversight bodies and parliament by taking the following steps:

    a. giving a designated parliamentary committee a role in the appointment of members;

    b. empowering parliament to task expert bodies to investigate particular matters;

    c. requiring that expert oversight bodies report and take part in hearings with a designated parliamentary committee.

On the effectiveness of oversight bodies

14. Guarantee that all bodies responsible for overseeing security services have access to all information, regardless of its level of classification, which they deem to be relevant to the fulfilment of their mandates. Access to information by oversight bodies should be enshrined in law and supported by recourse to investigative powers and tools which ensure such access. Any attempts to restrict oversight bodies' access to classified information should be prohibited and subject to sanction where appropriate.

15. Ensure that security services are placed under a duty to be open and co-operative with their oversight bodies. Equally, oversight bodies have a responsibility to exercise their powers, including seeking and handling classified information, professionally and strictly for the purposes for which they are conferred by law.

16. Ensure that access to information by oversight bodies is not restricted by or subject to the third party rule or the principle of originator control. This is essential for ensuring that democratic oversight is not subject to an effective veto by foreign bodies that have shared information with security services. Access to information by oversight bodies should extend to all relevant information held by security services including information provided by foreign bodies.

17. Require security services to proactively disclose to overseers (without being requested) information relating to areas of activity that are deemed to present particular risks to human rights, as well as any information relating to the potential violation of human rights in the work of security services.

18. Ensure that external oversight bodies – including parliamentary oversight committees and expert oversight bodies – are authorised by law to hire independent specialists whose expertise is deemed to be relevant. In particular, oversight bodies should have recourse to specialists in information and communications technology who can enable overseers to better comprehend and evaluate surveillance systems and thus to better understand the human rights implications of these activities.

19. Make sure that all institutions responsible for the oversight of security services have the necessary human and financial resources to fulfil their mandates. This should include recourse to technological expertise that can enable overseers to navigate, understand and evaluate systems for the collection, processing and storage of information. The adequacy of such resources should be kept under review and consideration should be given as to whether increases in security service budgets necessitate parallel increases in overseers' budgets.

20. Ensure that all oversight bodies with access to classified information and personal data (regardless of whether it is classified) put in place measures to make sure that information is protected from being used or disclosed for any purpose that is outside the mandate of the oversight body.

On transparency and engagement with the public

21. Require by law that external bodies responsible for scrutinising security services publish public versions of their periodic and investigation reports. Any such requirements should be accompanied by additional resources that enable oversight bodies to produce informative reports without undermining their core oversight functions.

22. Ensure that security services and their oversight bodies are not exempt from the ambit of freedom of information legislation and instead require that decisions not to provide information are taken on a case-by-case basis, properly justified and subject to the supervision of an independent information/data commissioner.

On reviewing oversight bodies and systems

23. Evaluate and review periodically the legal and institutional frameworks, procedures and practices for the oversight of security services. Evaluations should include but not be limited to examining:

    a. the legal mandate of oversight bodies;

    b. the effectiveness of oversight bodies in helping to ensure that security service policies, regulations and operations comply with national and international human rights standards;

c. the efficacy of oversight bodies' investigative techniques;

d. the implications of new technologies for oversight;

e. the adequacy of powers and tools to access classified information;

f. the protection of information by oversight bodies;

g. the relations and co-operation between oversight bodies;

h. reporting and public outreach.

24. Review the adequacy of arrangements for the oversight of the collection and retention of personal data by private companies, including communications providers, for national security purposes, as well as the co-operation between private companies and security services.

25. Review the legal framework for the oversight of computer network exploitation by security services and consider whether existing arrangements provide necessary safeguards under national and European human rights law.

Chapter 1

INTRODUCTION

Ongoing revelations by former US intelligence contractor Edward Snowden have brought renewed attention to the activities of security services in the member states of the Council of Europe. Concerns about the implications of large-scale electronic surveillance activities have once again given rise to questions about the adequacy of the oversight of security services. It is axiomatic that the oversight of security services is fundamental to ensuring that these institutions both contribute to the protection of the populations they serve (including their human rights) and respect the rule of law and human rights in undertaking this task. Yet the Snowden revelations, the involvement of some European security services in the secret detention and extraordinary rendition of terrorist suspects in the past decade and ongoing allegations of other impropriety in various countries have cast significant doubt on the capacity of national oversight systems to perform this role. Indeed, the Council of Europe Commissioner for Human Rights recently described democratic oversight of security services as being "woefully inadequate" in many European countries (Commissioner for Human Rights 2015: 26).

For the purposes of this issue paper, the term "oversight" is used broadly to include the scrutiny of security service activities, policies and regulations before, during and after they are implemented/adopted. This includes functions that are variously labelled as monitoring, scrutiny, review and evaluation. The term "control" is reserved for functions where the relevant body has a direct say in whether or not and/or how a given activity is undertaken by a security service. Oversight of security services is generally undertaken by a combination of the following actors: parliament; the political executive; the judiciary; expert oversight bodies; and bodies internal to security services. Together, these actors will be referred to as "oversight systems". For the purposes of this issue paper "external oversight" refers to oversight by institutions that are external to the security services and associated executive departments/ministries/ministers. In addition to the official oversight institutions, which are generally founded upon statutory or even constitutional law, civil society and the media also play an important role in the oversight of security services and in monitoring the work of oversight bodies.

The label "security service" refers to state bodies, including both autonomous agencies and departments/units of other government departments or the armed forces, that have a mandate to collect, analyse and disseminate intelligence within the borders of their state in order to inform decisions by policy makers, military commanders, police investigators and border/customs agencies about threats to national security and other core national interests. In some Council of Europe states, their functions may also include aspects of law enforcement and the protection of installations and persons. For these purposes, some security services also exercise coercive powers of arrest and detention. The oversight of these activities should be governed by the same principles that apply to law-enforcement personnel – this is not dealt with in any detail in this issue paper.

Compliance with human rights by security services depends not only on effective oversight but also on the legal frameworks governing their work. Numerous publications have addressed the application of the European Convention on Human Rights ("the Convention" or ECHR) to security service activity and put forward principles on the scope and conduct of their work.[1] This issue paper will not revisit these issues; it will not address what security services are permitted to do or how their work should be regulated. Instead, the purpose of this issue paper is to take stock of international standards on and national approaches to the oversight of security services with a view to identifying practices or procedures that can strengthen human rights protection in the work of security services. This will be done by first examining the international legal standards and soft-law principles that are relevant to oversight and by then considering national approaches to different aspects of oversight. Finally, this issue paper will consider a number of objectives for developing/improving a system of security service oversight. Before embarking on this assessment, the paper provides an overview of the human rights implications of some areas of security service activity in the Council of Europe area.

1. For example: UN 2010a; Cameron 2000; Omtzigt 2015.

Chapter 2

OVERVIEW OF THE IMPACT OF NATIONAL SECURITY SERVICES' ACTIVITIES ON HUMAN RIGHTS PROTECTION IN EUROPE

It has long been recognised that the work of security services affects a range of human rights and may also undermine broader democratic processes. Security services have a number of characteristics that create the potential for human rights abuses if these services are not subject to effective oversight and underpinned by effective laws. These characteristics include recourse to very invasive powers that can be used in a highly discretionary manner, undertaken largely in secret and, in some countries, viewed as an instrument of the incumbent government that can be used for political purposes.

The purpose of this chapter is to highlight some of the ways in which security services have impacted (and continue to impact) upon human rights in Council of Europe member states; it is not intended to provide an exhaustive analysis of the ways in which security service activity engages human rights. This overview is provided with a view to better illustrating why services need to be subject to robust systems of oversight. Throughout this chapter reference is made to the activity of security services. This should, however, be read as sometimes including members of the executive branch who direct, set policies for and, in some cases, task security services. In various Council of Europe states political executives have a long history of (ab)using their security services to undertake unlawful and anti-democratic activities.

This chapter will focus on a number of the most prominent examples of security service activity impacting upon human rights over the past 15 years. Yet it is important to recall that there is a long history of human rights violations by security services in Europe, many of which took place in an era during which security services were subject to far less regulation and oversight and where the amount of public information on security service activity was considerably lower than today. Prominent historical examples include the systematic human rights violations by security services such as the Stasi (in the German Democratic Republic), the Securitate (in Romania) and the STB (in Czechoslovakia). Violations of human rights were by no means confined to security services of what was then the Eastern bloc. Inquiries in other countries such as Luxembourg and Norway have revealed extensive and unlawful domestic surveillance, primarily of left-wing groups and individuals.

Contemporary examples of the impact that security service activities can have on human rights can be broadly grouped into four categories. First, there are activities that have impacted upon personal integrity including the right to life, the right to personal liberty and security, and the right not to be subjected to torture or inhuman, cruel and degrading treatment. Second, security service activities have implications for the right to privacy and family life. In most jurisdictions this is the most common way in which security services interfere with human rights. Third, security service activity impacts upon the rights to freedom of expression, association and assembly. Finally, brief consideration will be given to the impact on the right to a fair trial of security service activity and in relation to legal proceedings involving security services.

2.1. Personal integrity and liberty

Since the terrorist attacks on the United States in September 2001 ("9/11"), the Council of Europe region has witnessed a broad range of revelations regarding the activities of security services in the context of counter-terrorism. Broadly speaking, these revelations have arisen from American-led counter-terrorism activities in which at least 25 European security services and their governments have co-operated to some extent (Commissioner for Human Rights 2014b). Regarding the involvement of European security services in US-led counter-terrorism activities, it is now either confirmed or widely accepted that services of one or more Council of Europe states:

- hosted American-run secret detention facilities at which suspected terrorists were held incommunicado and subjected to mistreatment;[2]
- facilitated the abduction and rendering of persons to such facilities both in Europe and outside of Europe;[3]
- arranged for and/or took part in the interrogation of persons detained by non-European intelligence services, either in concert or alternation with these services.[4]

Such actions have violated, *inter alia*, Articles 3, 5, 6, 8 and 13 of the European Convention on Human Rights. A full exploration of these revelations is beyond the scope of this issue paper. It suffices to say that Council of Europe institutions (far more than national institutions) have played a pre-eminent role in investigating and providing remedies for these breaches of human rights. This has included Dick Marty's investigative reports for the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe (PACE) and the European

2. The Court has found against Poland in two cases: *Al Nashiri v. Poland*; *Husayn (Abu Zubaydah) v. Poland*. These judgments are now final after the Strasbourg Court refused permission to have them referred to its Grand Chamber. There are pending cases against Romania (*Al Nashiri v. Romania*) and Lithuania (*Abu Zubaydah v. Lithuania*). See also: European Parliament 2013 and Connolly 2014.
3. See for example: *El Masri v. "the former Yugoslav Republic of Macedonia"* and *Nasr and Ghali v. Italy*. See also: Open Society Justice Initiative 2013: 78 (Georgia), 109 (Sweden).
4. See for example: Human Rights Watch 2009: 17-35; Cobain 2013: 240-242, 253, 257-258 and Open Society Justice Initiative 2013: 78 (Germany).

Court of Human Rights' landmark decisions in the cases of *Al Nashiri v. Poland*, *Husayn (Abu Zubaydah) v. Poland* and *El Masri v. "the former Yugoslav Republic of Macedonia"*.

In addition to the violation of human rights in the context of US-led counter-terrorism activities, there have also been allegations of torture, inhuman and degrading treatment, arbitrary detention and the unlawful use of lethal force by Russian security forces, particularly in Chechnya and Dagestan.[5]

It has also been widely alleged that European security services have been complicit in the violation of the rights not to be tortured and/or arbitrarily detained through their provision of information to foreign partners. Although the implications of such information have been difficult to verify, it is likely to have included providing: information or questions that have been put to persons being detained and tortured by non-European security services;[6] information to US intelligence services that may have been used in identifying and locating persons for extrajudicial killing;[7] and information that has led to the extraordinary rendition of persons and/or arbitrary detention by non-European intelligence services.[8]

Beyond activities relating to international intelligence co-operation, there have been allegations that in some parts of the Council of Europe area security services continue to be involved in arbitrary arrests and incommunicado detention.[9] It is in this area that the secrecy and high levels of discretion that characterise security service work pose a particular threat to personal integrity.

2.2. Right to privacy and family life

Security services are mostly likely to impact upon the right to privacy and family life through the collection, retention and transfer of personal data.[10] It is not only the actual use of these measures against given individuals that infringes the right to privacy but also their potential use and/or the mere existence of legislation permitting their use.[11] The right to privacy can of course be lawfully restricted by security services as long as this complies with requirements under national law and the ECHR.

---

5. See for example: UN 2010b: paragraphs 208-214 and Nemtsova 2012.
6. Cobain 2013: Chapter 8.
7. See for example: Singh and Scholes 2014; Stark 2011; Osborne 2013.
8. See for example the ongoing UK case of Abdul Hakim Belhaj: www.reprieve.org.uk/case-study/abdul-hakim-belhaj/, accessed 28 March 2015.
9. For example: Commissioner for Human Rights 2013a: § 8.
10. Confirmed by the European Court of Human Rights with respect to the following activities: telephone (*Malone v. the United Kingdom* [64]); e-mail (*Weber and Saravia v. Germany* [77]); storage of information in security service registers (*Segerstedt-Wiberg and Others v. Sweden* [72]); failure to advise a person about information being kept on them (*Segerstedt-Wiberg and Others v. Sweden* [99]); storage and use of personal data by security services (*Leander v. Sweden* [48]); transmission to and use by other authorities constitutes a separate interference (*Weber and Saravia v. Germany* [79]); provisions for destruction and failing to notify (*Weber and Saravia v. Germany* [79]); installation of listening devices (*Vetter v. France* [20]).
11. *Weber and Saravia v. Germany* [78-79]; *Liberty and Others v. the United Kingdom* [57].

Historically, concerns about the impact of the right to privacy arose primarily from security services' use of targeted surveillance through means such as tapping an identified individual's telephone or placing listening devices in his/her dwelling. That is, measures that focus on a given person or organisation, usually on the basis that there is reasonable suspicion that they are either engaged in serious criminal activity or otherwise threaten national security. Human intelligence collection, including the recruitment of informants and infiltration of groups, is another feature of security service work that has long impacted upon the right to privacy. Although such activities continue to be used and impact on the right to privacy, concerns about them have, in many parts of the Council of Europe area, been supplanted by revelations about untargeted, bulk collection of electronic communications.

Rapid technological development has given security services in some Council of Europe member states the possibility to conduct more extensive surveillance of communications while expending fewer human resources. In Europe, bulk interception by security services first gained public attention with the "Echelon" revelations at the turn of the century (European Parliament 2001). Far more significant are the disclosures by former US intelligence contractor Edward Snowden, which commenced in the summer of 2013. Snowden has revealed large-scale surveillance of electronic communications and Internet activity by the US National Security Agency and various security services in Europe. Revelations of similar programmes have also emerged in France, for example.[12]

Unlike more traditional forms of surveillance, the programmes revealed do not necessarily target specific individuals or organisations on the basis of a suspicion that they are involved in particular activities. Instead, they broadly entail the automated interception (using a variety of tools and sometimes with the assistance of communications providers) of huge swathes of information passing through fibre-optic cables or wireless communications, or held by third parties. Information gathered includes the content of communications as well as so-called communications data or metadata such as email addresses, IP addresses, phone numbers and locations of phones. Information collected is later searched or "mined", using particular selectors or search terms designed to extract information relating to persons/organisations of interest to security services.[13]

The Snowden revelations have generated serious concern about the right to privacy and family life. The activities revealed have been the subject of investigations by the European Parliament (EP), the PACE Committee on Legal Affairs and Human Rights (through its rapporteur Pieter Omtzigt) and various national oversight bodies. They have been challenged through the courts both domestically[14] and at the Strasbourg Court.[15]

---

12. Follorou and Johannès 2013; Follorou 2014; Bigo et al. 2014.
13. For an overview see: Venice Commission 2015: §§ 48-51; Bigo et al. 2013; Omtzigt 2015.
14. See for example, Privacy International in the UK: www.privacyinternational.org/?q=legal-actions, accessed 28 March 2015.
15. *Big Brother Watch and Others v. the United Kingdom*.

Commenting on revelations about bulk surveillance UN Special Rapporteur Ben Emmerson has stated that:

> The very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy … it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. [These programmes are] a direct and ongoing challenge to an established norm under international law. (UN 2014: §§18 and 59)

The UN High Commissioner for Human Rights expressed similar concerns about the justification for such interferences with the right to privacy, stating:

> It will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate. (UNHCHR 2014: §25)

Finally, the incumbent Council of Europe Commissioner for Human Rights has described this bulk surveillance as a "severe threat to the right to privacy" (Commissioner for Human Rights 2013b).

The right to privacy is engaged not only by the interception of the content of communications but also by the collection, retention and use of so-called communications data or metadata.[16] Although communications data may be gathered and retained directly by security services, in most states private sector communications providers are required by law to retain customers' communications data for a defined period. In April 2014, the Court of Justice of the European Union (CJEU) held that the EU's data retention directive, which mandated the retention of communications data by communications providers for law-enforcement purposes, was incompatible with the right to privacy.[17] Commenting on the privacy implications of communications data, the CJEU held that:

> [Communications] data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[18]

In many Council of Europe member states, bulk, untargeted surveillance by security services is either not regulated by any publicly available law or regulated in such a nebulous way that the law provides few restraints and little clarity on these measures. This is problematic from a human rights perspective because it makes it difficult for individuals and organisations to understand the legal basis and reasons for which their communications may be intercepted, or to challenge such surveillance as being unlawful (Commissioner for Human Rights 2014a: 109-110).

---

16. See further: Commissioner for Human Rights 2014a: 115-117.
17. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others,* see in particular [29] [57] [58] and [65].
18. Ibid. [27].

Computer network exploitation (CNE – colloquially known as hacking) is another area of security service activity that poses a significant risk to human rights. CNE includes practices as diverse as placing malware or Trojans on IT systems as a means of extracting information; exploiting cameras and microphones within computers or hand-held devices to record the users' activities; and infiltrating electronic devices to manipulate the content of communications sent from/to them.[19] This remains a relatively new area of activity and one that is neither addressed explicitly in security service legislation nor covered in any detail in public reporting on security services' work. It is nevertheless clear that such activities pose a grave threat to the right to privacy and family life. CNE is potentially more intrusive than the interception of the content of communications and/or metadata, not least because it enables access to information which a person may never have chosen to share with anyone. In a submission to the UK's Investigatory Powers Tribunal, Privacy International captures the threat to privacy by stating:

> The modern equivalent of entering someone's house, searching through his filing cabinets, diaries and correspondence, and planting devices to permit constant surveillance in the future, and, if mobile devices are involved, obtaining historical information including every location he visited in the past year … if a mobile device has been infected, the ongoing surveillance will capture affected individuals wherever they are. (Privacy International 2014: §§ 4-6, 11-18)

Taking the example of exploiting a smartphone's microphone and camera to record a person's ongoing interactions and surroundings, this would undoubtedly be more invasive than placing listening devices in a home or car and/or following that person with human agents. CNE may also create vulnerabilities in systems that could be exploited by third parties such as organised criminal groups.

Alongside concerns that international intelligence sharing could lead to persons being subject to torture and arbitrary detention, cross-border exchanges of personal data by security services also have implications for the right to privacy. This right is engaged each time personal data are transmitted. Particular concerns arise where foreign security services to which information is sent do not have the same standards of data protection and/or or stringent legal requirements limiting the use of personal data for specific purposes. Although many security services attach caveats (requirements on how information can be used) to outgoing information, these cannot fully mitigate possible violations of the right to privacy by the recipient. A further issue is the deliberate or accidental use of international intelligence sharing to circumvent the safeguards that would ordinarily apply to the collection of information. While security services would usually have to obtain a warrant to, for example, intercept a person's communications within their country, if this same information were gathered by a foreign partner and later shared it is possible that no such safeguards would apply. Such risks are heightened in the context of intelligence sharing relationships that include automated sharing of electronic data and/or integrated systems collecting and storing information gathered by more than one state.[20]

---

19. For an overview, see: Omtzigt 2015: §§ 66-69; Gallagher and Greenwald 2014; BBC News 2015.
20. For an overview, see: Venice Commission 2015: § 78.

2.3. Rights to freedom of expression, assembly and association

Security service activity impacts upon the rights to freedom of expression, assembly and association, which are rights designed to protect interactions with other people. Interference with these rights can have broader implications for processes that are integral to the functioning of a democracy and the rule of law, including a free press, the operation of political parties, trade unions, religious organisations and the work of human rights defenders.

Interference with these rights may be direct or indirect. Security services sometimes interfere directly with the right to freedom of expression by, for example, forcing media outlets to change their editorial line (Human Rights Watch 2014a: 25), seeking to prevent the publication of information,[21] requiring organisations to remove information that has been published online,[22] forcing organisations to delete information that may be (further) published (Borger 2013), and seizing information from journalists.[23] Such measures may sometimes represent lawful limitations on human rights; however, they are also taken in a manner that is not ECHR-compliant.

Equally significant is the use of powers (such as those held by Russia's security services) that permit security services to issue warnings to persons whose conduct (including publications or speech) is deemed to be undesirable but has not yet crossed the threshold of being a criminal offence.[24]

Indirect interference with rights to freedom of expression, association and assembly results primarily from surveillance, including both targeted and untargeted measures, and (increasingly) CNE by security services. Security service monitoring (potential or actual) of a person's communications, expressions of thought and discussions may have a chilling effect on the exercise of these rights because it impacts upon that person's willingness to engage in these interactions and may shape the content of such interactions. Responding to revelations about mass surveillance of Internet-based activities, the UN High Commissioner for Human Rights has observed that these rights are all affected because they are rights that are increasingly exercised through digital media (UNHCHR 2014). In this regard, there is a strong link between the right to privacy and family life and the freedoms of expression, association and assembly. Privacy enables individuals to realise these other rights without unlawful interference (UN General Assembly 2013).

The chilling effect of (potential) surveillance arises not only from the interception of the content of communications or discussions but also, as the CJEU has recently recognised, laws mandating the retention of communications data/metadata.[25] The European Court of Human Rights has recognised that it is not only the actual

21. *Sunday Times v. the United Kingdom (No. 2)*.
22. For example: *Le Monde* 2013.
23. See, for instance, the David Miranda case in the UK: www.bbc.co.uk/news/uk-23782782, accessed 28 March 2015.
24. See for example the Venice Commission's discussion of this power in Russia: Venice Commission 2012: §§ 48-61.
25. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* [28].

implementation of surveillance measures that impacts on the right to freedom of expression (and, by analogy, association and assembly) but the mere existence of legislation permitting such measures constitutes an interference.[26] Beyond the collection of information, the Court has recognised that the processing of personal data engages not only the right to respect for private and family life, but also freedom of thought, conscience and religion, of expression, and of assembly and association when such data are processed with regard to a person's political opinion or membership of given groups.[27]

In some parts of the Council of Europe area, security services continue to be used as instruments by a ruling party or incumbent heads of government/state. Such interference takes a variety of forms. At its most blunt form, it includes harassment (or even physical attacks) by security services of persons/organisations deemed to be critical of the government, as well as direct interference in political processes (Commissioner for Human Rights 2013a: §39). More commonly, security services eavesdrop on opposition politicians, NGOs and judges (at the request of the political executive or of their own volition) as means for uncovering information to smear persons regarded as opponents and/or to intimidate them. Such allegations have been made, for example, in "the former Yugoslav Republic of Macedonia" and Serbia (Balkan Insight 2015a). Activities of this nature undermine democratic processes and the rule of law. Finally, there have also been cases where security services have carried out unauthorised surveillance against members of the executive branch (Higgins 2013). This is particularly problematic given that democratic governance requires that security services are under civilian control and do not become a state within a state.

Especially concerning is the impact of security service surveillance of media organisations, whose functions include holding governments to account for their security policies and activities. Surveillance can serve to undermine the confidentiality of journalists' sources and, in turn, the ability of journalists to uncover wrongdoing in government.[28] Such work is especially important given that, in many states, official oversight bodies have not been effective in detecting and responding to human rights violations by security services.

2.4. Right to a fair trial and the right to an effective remedy

Security service activity can undermine the right to a fair trial and the right to an effective remedy in a variety of ways. First, it is often extremely difficult for individuals to bring civil claims against security services even if they are aware that their rights have potentially been violated. This is because governments and security services may invoke state secrecy arguments to prevent challenges being heard or rely on "neither confirm nor deny" (relating to their agents and activities) policies to frustrate legal proceedings.

26. *Weber and Saravia v. Germany* [144].
27. *Segerstedt-Wiberg and Others v. Sweden* [107].
28. *Weber and Saravia v. Germany* [143] [145]; see also: European Parliament 2014: §§ 86-87.

Second, where challenges can be brought, judicial proceedings may be significantly amended in order to safeguard classified information. Such modifications to proceedings can make it difficult or impossible to have a fair trial. For example, parties and their legal representatives may be excluded from all or parts of proceedings making it difficult to know, let alone meet, the case against them. There may also be limited or no rights to be given reasons for a judgment and very restricted rights of appeal.

Third, the interception of communications between lawyers and their clients, as was recently revealed in the UK, can undermine the equality of arms and the right to a fair trial especially where security services are party to the litigation concerned (Travis and Bowcott 2015).

Fourth, the exchange of information with foreign security and law-enforcement bodies can pose a risk to the right to a fair trial. Regarding information transmitted to foreign bodies, there is a risk that it may be used (contrary to warnings regarding reliability or its not being used in legal proceedings) in criminal or other proceedings. Information received from foreign bodies, which may have been obtained in violation of human rights or is otherwise unreliable, may in some states be used in legal proceedings, thereby rendering them unfair.

Finally, some states have adopted laws that give members of security services *de facto* immunity from prosecution and/or civil claims. In Turkey, for example, members of the security services cannot be prosecuted without the permission of the prime minister and minister of the interior.[29] Such provisions have the potential to promote impunity in relation to human rights violations.

29. Turkey 2014; Human Rights Watch 2014b.

Chapter 3

OVERVIEW OF INTERNATIONAL AND EUROPEAN STANDARDS CONCERNING DEMOCRATIC OVERSIGHT OF NATIONAL SECURITY SERVICES

International and European standards on the oversight of security services can be broadly divided into binding legal instruments (hard law) and non-binding principles or recommendations (soft law). The former category includes a number of international and regional treaties, as well as their interpretation by relevant courts or treaty bodies. The latter category includes recommendations, resolutions, declarations and reports from four sources: (i) UN institutions; (ii) Council of Europe institutions; (iii) the European Union; (iv) civil society-led transnational initiatives.

3.1. International and regional legal instruments

There are no international treaties that explicitly deal with the oversight of security services. However, the International Covenant on Civil and Political Rights (ICCPR),[30] the UN Convention Against Torture (UNCAT) and the ECHR all include articles that are pertinent to states' obligations surrounding the oversight of security services. All Council of Europe member states are bound by these treaties.

30. International Covenant on Civil and Political Rights, 16 December 1966 (entry into force 23 March 1976).

Particular oversight requirements under Article 8 of the ECHR (Right to respect for private and family life)

Article 8 of the ECHR has been interpreted as implying a number of requirements for the oversight of security services. Through its Article 8 jurisprudence, the Strasbourg Court has set out criteria on what is required (as a minimum) in terms of oversight in order for security service measures that infringe the right to privacy and family life to be ECHR-compatible. The Court has also given guidance on the factors that are likely to be assessed on a case-by-case basis when evaluating whether or not a given oversight system affords sufficient safeguards. This jurisprudence has primarily been developed on the basis of challenges brought against targeted and untargeted surveillance measures, the retention of personal data by security services and attempts by individuals to verify whether security services hold their personal data. The principles discussed here could nevertheless apply to the oversight of other measures that engage Article 8 of the Convention. Notably, they are likely to cover CNE in situations where these measures engage the right to privacy. While they are not discussed in this paper, it should be noted that security service activities also need to comply with other requirements set out in Article 8(2) and its jurisprudence, which are not specific to oversight (Venice Commission 2007, 2015).

The Court has emphasised the critical importance of external supervision for safeguarding against the abuse and arbitrary use of intrusive measures. It has pointed out that the external oversight of surveillance measures may take place before measures are implemented, during their implementation or following their termination.[31] These latter stages are often combined as one single stage, distinct from the authorisation of intrusive measures.[32]

Regarding the authorisation of surveillance measures, the Court has expressed a clear preference for surveillance to be authorised by a judicial body but it has stopped short of making this a requirement in order for them to be Article 8-compliant.[33] Bodies tasked with authorising intrusive measures must be independent of the relevant service and the executive.[34] The Court has made it clear that these safeguards apply equally to the authorisation of targeted and untargeted surveillance.[35] When assessing whether a given body or system provides sufficient safeguards at the authorisation stage, the Court may have regard to their powers and competences,[36] as well as to the number of authorisations granted on an annual basis.[37]

The European Court of Human Rights has also ruled on *ex post* oversight arrangements, indicating that there may be a violation of Article 8 if there is not a genuinely independent body involved in the *ex post* review of surveillance measures and the

31. *Klass and Others v. Germany* [54].
32. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* [84]. See also: Cameron 2013: 170-171.
33. *Klass and Others v. Germany* [54] [56]; *Kennedy v. the United Kingdom* [167].
34. *Dumitru Popescu v. Romania* [72][73]; *Klass and Others v. Germany* [56].
35. *Liberty and Others v. the United Kingdom* [64].
36. *Klass and Others v. Germany* [56].
37. *Iordachi and Others v. Moldova* [51].

retention and destruction of personal data by security services.[38] There must be a clear legal basis setting out how any such supervision is carried out.[39] Finally, the Court has identified a number of additional attributes of oversight bodies as being relevant to an assessment of whether or not oversight arrangements provide sufficient safeguards. These include whether or not the overseer has access to all relevant documents (including classified material); whether public reports are produced (subject to appropriate restrictions on classified material); and whether an oversight body has the power to quash warrants/orders for surveillance and require material obtained to be destroyed.[40]

Beyond the Court, in a 2014 decision that is binding on the 28 Council of Europe member states that are also members of the EU, the Grand Chamber of the Court of Justice of the EU indicated that, in relation to access to communications data by state bodies, there is a need for:

> Prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.[41]

It should be noted that this decision was made within the specific context of assessing the legality of the EU's data retention directive, which required data to be retained primarily for law-enforcement purposes. Additionally, national security and the activities of security services are largely outside the ambit of EU law. Nevertheless, the CJEU's decision provides a strong indication that *ex ante* independent authorisation of requests to access communications data is a requirement in order for the exercise of such powers to be compatible with the right to privacy. Similar reasoning will almost certainly apply as and when such measures, including in relation to security services, are considered under Article 8 of the ECHR.

Investigating human rights violations and providing effective remedies

States are required to ensure that individuals have recourse to an effective remedy for violations of their rights (Article 13 ECHR; Article 2(3) ICCPR and Articles 13 and 14 UNCAT). This has clear implications for the oversight of security services as one or a combination of the institutions responsible for their oversight must investigate allegations of human rights violations and ensure that victims are provided with an effective remedy. The importance of providing an effective remedy has been confirmed by the UN Human Rights Committee which has stated that the failure to investigate allegations of violations of human rights could in itself constitute a separate breach of the ICCPR (UN Human Rights Committee 2004: § 15). In the context of allegations relating to torture, UNCAT lays down more detailed requirements

38. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* [85] [87].
39. *Iordachi and Others v. Moldova* [49].
40. *Kennedy v. the United Kingdom* [166] [167].
41. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* [62].

including the "systematic review of interrogation rules, instructions, methods and practices as well as arrangements for the custody and treatment of persons subjected to any form of arrest, detention or imprisonment" and the undertaking of prompt investigations into allegations of torture.[42]

In countries where security services are permitted to question and/or detain people (or do so without a legal basis), these obligations are likely to be especially relevant. It is not regarded as good practice for security services to exercise powers of arrest, interrogation and detention and recourse to such powers should not be permitted if services do not have any law-enforcement functions. In any circumstances in which services do exercise such powers, it is regarded as essential for them to be subject to the same standards as those applied to law-enforcement bodies exercising similar powers.[43]

Article 13 of the ECHR and its jurisprudence imposes similar requirements for investigating and remedying human rights violations by security services. Additionally, the Court has ruled that, where an individual has an arguable claim against security services (or any other state actor) in relation to a violation of either Article 3 or 5, the relevant article must be read together with Article 13 to require an effective official investigation.[44] This demands that serious attempts are made to find out what happened, all reasonable steps are taken to secure evidence, the victim is permitted to participate effectively in the investigation and that any investigation must be independent from the executive.[45]

The Court has long recognised that the concept of effective remedy cannot carry the same meaning in the context of secret intrusive measures because the efficacy of such measures depends upon their remaining secret. In view of this, the Court has accepted that, as long as secret surveillance measures are either ongoing or cannot be revealed to the subject for other legitimate reasons, remedies need only be as effective as they can be given the circumstances.[46] However, the Court has held that the fact that a person cannot be informed as to whether or not they are under surveillance or have been under surveillance should not preclude them from being able to raise a complaint with an oversight body. Such a body should be able to conduct investigations to ensure that any measures are being used in accordance with the law, without informing the complainant one way or the other.[47] Once measures are known to the subject, as a result of a legal requirement to notify him/her, or they are otherwise revealed, he/she must have recourse to a body that can provide an effective remedy. The Court has emphasised that such remedies must be effective not only in law but also in practice.[48]

---

42. UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 10 December 1984 (entry into force 26 June 1987), Articles 11-12.
43. UN 2010a: practices 27-28; International Commission of Jurists 2009: 89.
44. *Assenov and Others v. Bulgaria* [102]; *El Masri v. "the former Yugoslav Republic of Macedonia"* [182] [242].
45. *Assenov and Others v. Bulgaria* [102-103]; *El Masri v. "the former Yugoslav Republic of Macedonia"* [182-184].
46. *Klass and Others v. Germany* [69].
47. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* [100].
48. *Segerstedt-Wiberg and Others v. Sweden* [117]. See also: Venice Commission 2007: § 129.

In common with requirements for the oversight of surveillance measures (discussed above), it is not strictly necessary for the body responsible for investigating complaints and providing remedies to be a judicial body. Such bodies must nevertheless possess sufficient powers and procedural guarantees to ensure that remedies are effective.[49] In particular, whether or not a body has the power to order legally binding remedies (rather than recommendations) is relevant to an assessment as to whether or not it is effective for the purposes of Article 13.[50] The power to order the destruction of files or the erasure of information collected is an essential corollary of this.[51] An assessment of whether there is an effective remedy can take account of the aggregate of remedies available,[52] which may be afforded by different bodies.

3.2. Non-binding recommendations and principles

There is a growing array of international and European soft law on the oversight of security services. While there are relatively few binding, hard-law principles applicable to oversight, non-binding proposals and endorsements provide a detailed framework for developing, enhancing and evaluating systems for the oversight of security services. Many of the documents discussed in this section carry significant weight given that they have been promulgated by major international institutions and are based on existing good practices rather than being "aspirational". This section will refer to a number of key provisions and innovations from each set of principles.

3.2.1. United Nations

Special mandate holders and High Commissioner for Human Rights

In 2009 the UN Human Rights Council mandated the Special Rapporteur on the protection and promotion of human rights while countering terrorism to produce a "compilation of good practices on the legal and institutional frameworks for intelligence agencies and their oversight" (UN Human Rights Council 2009; UN 2010a). It was developed in consultation with a broad range of stakeholders including former intelligence officials, human rights lawyers and with the inputs from many national governments. These principles have subsequently been endorsed by the European Parliament and the Parliamentary Assembly of the Council of Europe.

The UN compilation includes notable recommendations on oversight including recognition of the importance of specialised oversight (referred to as expert oversight in this issue paper), in addition to parliamentary, judicial, executive and internal oversight and control. The compilation also highlights the importance of there being an oversight institution responsible for scrutinising the use of personal data by intelligence agencies and for receiving complaints about such matters

49. *Klass and Others v. Germany* [67]; *Segerstedt-Wiberg and Others v. Sweden* [117]; *Leander v. Sweden* [83].
50. *Leander v. Sweden* [82].
51. *Segerstedt-Wiberg and Others v. Sweden* [120]; *Kennedy v. the United Kingdom* [167].
52. *Klass and Others v. Germany* [72]; *Leander v. Sweden* [77].

(UN 2010a: practices 25-26). Equally important is the recommendation on the need for a holistic focus on services' activities, with oversight covering (as a minimum):

- compliance with the law;
- the effectiveness and efficiency of their activities;
- their finances; and
- their administrative practices. (UN 2010a: practice 6)

Finally, the recommendation that an oversight body must be in a position to scrutinise co-operation with foreign intelligence and security services (including co-operation agreements) is important in view of the exponential growth of co-operation and the human rights implications of such co-operation (Born, Leigh and Wills, forthcoming).

In 2014, the UN Special Rapporteur on human rights and counter-terrorism put forward recommendations on the oversight of bulk surveillance, which included the following.

- An independent oversight body should be mandated to authorise surveillance (including bulk surveillance), taking account of not only domestic law but also the international human rights law requirements of necessity and proportionality.
- The need for individuals to have access to an effective remedy for alleged violations of online privacy rights. It is stressed that bodies responsible for handling such complaints can take different forms as long as they have access to all relevant information, adequate resources and can order binding remedies (UN 2014: §§ 48-50 and 61). This acknowledgement that the substance and not the form of oversight bodies matters is significant in devising principles of application to states with diverse constitutional/legal systems – it is also consistent with the approach taken in the UN compilation.

The 2013 recommendations of the UN Special Rapporteur on the freedom of expression go further, calling for the surveillance of communications to only take place under the supervision of a judicial authority (UN 2013: § 81). This goes beyond the ECHR requirements developed through case law (see above). Frank La Rue also recommended that the provision of communications data to state agencies, including security services, by private companies should be monitored by an independent oversight body or a court (UN 2013: § 86).

The UN High Commissioner for Human Rights published a report in 2014 suggesting that authorisation processes include "public interest advocacy positions". These are advocates appointed to represent the interests of would-be targets of surveillance (UNHCHR 2014: § 38).

UN General Assembly

The UN General Assembly in 2014 responded to the Snowden revelations by calling upon states, *inter alia*, to:

> Establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance

of communications, their interception and the collection of personal data; provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations. (UN General Assembly 2014: § 4)

3.2.2. Council of Europe

Venice Commission

The Council of Europe's Venice Commission has played a leading role in promoting the democratic control of security services. The Venice Commission's 1998 report on the internal security services was the first document produced by an international organisation on the subject (Venice Commission 1998). Through a comprehensive report in 2007, the Venice Commission has provided comprehensive analysis of different forms and models of oversight. The report includes detailed discussion of internal, parliamentary, judicial and expert oversight.

The Venice Commission identifies the need for effective internal controls within security services, including management control of lower ranks, procedures for ensuring that requests for authorisations of intrusive measures are approved at management level, and training on human rights and democratic values (Venice Commission 2007: §§ 131-133). Regarding parliamentary oversight, the Venice Commission recommends that: parliament (not the executive) should select committee members, there should be cross-party representation and there should be support staff with adequate expertise (ibid. §§ 21, 24). With respect to judicial oversight, the Venice Commission recommends specialist training for judges on security matters and that consideration be given to the appointment of special advocates to represent would-be targets of surveillance in the context of authorisation proceedings (ibid. §§ 28, 31). Recommendations on expert oversight bodies include the suggestion that parliament (not the executive) should appoint their members and receive their reports, and the avoidance of government control of reporting functions (ibid. § 34). It is also recommended that complaints-handling functions be separated from broader oversight functions (ibid. § 247). Finally, the report also issues an important reminder that it is insufficient for oversight mechanisms to exist on paper – they must be implemented and kept under review (ibid. § 260). No guidance is offered though on how such reviews should be done.

In 2015, the Venice Commission updated this report in light of the Snowden revelations (Venice Commission 2015). The report provides detailed recommendations on the safeguards and oversight mechanisms that can be adapted for use with untargeted surveillance and the use of metadata. The Venice Commission has highlighted the special need for safeguards to be instituted at two stages.

- When selectors are chosen to determine the information that is extracted from material collected through bulk surveillance. It is recommended that, although this could be authorised by a judicial body, it is a task that may be best suited to a hybrid external body of experts and judges because it involves not only legal assessments but (foreign) policy and technical considerations.
- When human analysts make the decision on whether the information gathered

through untargeted surveillance and extracted through selectors should be retained – the minimisation process. The Venice Commission recommends that this function should be overseen *ex post* by an external body. (Venice Commission 2015: §§ 46-48, 120-121)

Parliamentary Assembly of the Council of Europe (PACE)

The PACE has also promulgated principles on the oversight of security services in the form of resolutions, recommendations and committee reports. These have emerged from the work of the Committee on Legal Affairs and Human Rights on secret detention, rendition, mass surveillance and state secrecy. As an assembly of parliamentarians from 47 European states, PACE has unsurprisingly focused its recommendations on the need for enhanced parliamentary oversight, recommending, *inter alia*, that all parliaments establish specialised committees for the oversight of security services.[53]

The Assembly has taken a particular interest in access to information by ad hoc and standing parliamentary committees, reaffirming the need for parliamentary committees to have access to all information relevant to the discharge of their functions as well as robust investigatory powers to pursue such material (PACE 2013: § 9). In its recent draft resolution, the Committee on Legal Affairs and Human Rights emphasised the need for oversight mechanisms to have access to information relating to (and be empowered to review) international co-operation between security/intelligence services without regard to the originator control principle.[54] This is especially important given vast amounts of information received and retained from foreign partners.[55] The Assembly has also recommended that member states institute special adversarial procedures to arbitrate in relation to disputes concerning the publication of information by parliamentary committees (and judicial bodies investigating matters involving security services) (PACE 2011: § 13). This specific aspect of oversight body transparency has not been addressed by other sets of principles and it represents a valuable addition because there are frequently impasses regarding what an oversight committee can publish and how any disputes with the executive should be resolved. Perhaps the most innovative recommendation made by the Assembly was its suggestion in 2005 that the Committee of Ministers adopt a code of ethics for security services along the lines of the European Code of Police Ethics (PACE 2005: § 10.i.*e*). Although this recommendation has not yet been acted upon, it remains an important aspiration which should be reconsidered.

Former PACE member, Dick Marty, used his final report to endorse the principles in the aforementioned UN compilation (UN 2010a) and those set out by the Venice Commission in its 2007 report on the democratic oversight of security services (Marty 2011: §§ 48-49). Marty also recommended that oversight bodies be given robust investigative powers that enable them to scrutinise the activities of security services

53. PACE 2011: § 13; PACE 2005: § 10.i.*b*.
54. According to this principle, the service from whom the information in question has originated has the right to determine with whom this information is shared.
55. Omtzigt 2015; LAHRC 2015: § 17.2.

even where such scrutiny is resisted by government. Additionally, he underlined the often-cited importance of oversight bodies being properly resourced and being fully independent from the executive (Marty 2011: § 55).

Commissioner for Human Rights

The Commissioner for Human Rights has also made recommendations relating to the oversight of security services in response to revelations about mass surveillance. He has emphasised the importance of fostering a culture of respect for human rights and the rule of law within security services in order to have an effective system of democratic oversight (Commissioner for Human Rights 2014a: 22). This links into the need to focus on internal management and controls, as highlighted by the Venice Commission. The Commissioner has also used his country visits to make recommendations including stating that the legal framework for the oversight of security services should cover new surveillance technologies (Commissioner for Human Rights 2014c: 71-72). This is a particularly pertinent recommendation because one of the reasons why some oversight bodies have struggled to address the problems created by bulk surveillance and CNE is that they are not equipped to oversee security service activities based on evolving technologies.

Secretary General

Completing the contributions from Council of Europe institutions, the former Secretary General of the Council of Europe, Terry Davis, also put forward recommendations on oversight in 2006. This occurred in the context of the revelations about secret detention and extraordinary rendition in Europe. Davis highlighted the lack of scrutiny of the activities of foreign services (on the territory of Council of Europe member states) by oversight bodies.[56] Although he offered little detail as to how this might be done, this is a subject of oversight that has not been covered by other sets of recommendations and principles.

3.2.3. European Union

European Parliament

In its 2014 report on mass surveillance (European Parliament 2014: §§ 74-79), the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) promulgated recommendations on oversight at the national level (European Parliament 2007). The committee called for what it labelled "meaningful oversight" to be conducted by a parliamentary and/or expert oversight body. This recognition of expert oversight further demonstrates the shift towards a more pluralistic understanding of oversight – beyond parliamentary and judicial oversight. In view of the challenges surrounding the oversight of bulk surveillance of electronic communications, the committee highlighted the need for overseers to be afforded

56. Council of Europe 2006a: § 101(iv); Council of Europe 2006b: §§ 46 and 68.

sufficient technical capacity, expertise and resources. In this context, members called for oversight bodies to be given the power to conduct on-site visits as an investigative tool.

The LIBE Committee also recommended that oversight bodies be required to engage with the public through reporting. This is especially important because overseers have a key role to play in explaining the work of services to the public and, where warranted, fostering public confidence. Finally, with regards to the oversight of surveillance in particular, MEPs highlighted the need for both *ex ante* and *ex post* oversight; this is consistent with the approach taken by the Court (European Parliament 2014).

Drawing all of this together, the LIBE Committee has called for the creation of a high-level group to develop minimum standards on oversight in the EU based on the principles and best practices put forward by the UN and the Council of Europe (European Parliament 2014: § 77). At the time of writing there have been no further announcements in this regard.

"Article 29 Working Party"

Also under the auspices of the European Union, the "Article 29 Working Party", which includes representatives of national data protection commissions, adopted in 2014 a declaration of European values on the protection of personal data in the context of national security surveillance. The declaration includes a call for independent and effective supervision of surveillance activities including the genuine involvement of national data protection authorities (DPAs) (European Data Protection Authorities 2014: § 8). In an earlier opinion, the Working Party recommended that in states where an oversight body other than the national data protection authority oversees the use of data protection by security services, there should be "regular contacts between this body and the national data protection authority to ensure a coherent and consistent application of the data protection principles" (Article 29 2014a: § 8). This is significant because in many Council of Europe member states DPAs are excluded from the oversight of security services (see below) and therefore their protection expertise is not brought to bear in a field in which data protection is highly complex.

Whichever body is responsible for overseeing the use of personal data, the "Article 29 Working Party" emphasises the need for it to be both permitted to examine matters on its own initiative and required to respond to complaints, as well as empowered to enforce its findings (Article 29 2014a: § 8, Recommendation B2). Finally, the "Article 29 Working Party" has also recommended that personal data should be organised and stored in a way to facilitate independent oversight (Article 29 2014b: § 11). This recognises that effective oversight depends not only on the powers and resources of oversight bodies but also on how institutions, such as security services, can facilitate oversight and accountability through their management of data.

3.2.4. Civil society initiatives

Civil society-led initiatives have developed various significant sets of international principles that are relevant to the oversight of security services.

Tshwane Principles

Launched in 2013, the Global Principles on National Security and the Right to Information (Tshwane Principles) were developed through the input of more than 500 experts worldwide, including numerous security professionals, under the auspices of the Open Society Justice Initiative (Open Society Foundations 2013). The Tshwane Principles set out detailed guidance on access to information by bodies that oversee the security sector, including security services. Starting from the principle that overseers should have access to all information necessary for the fulfilment of the legal mandates, the principles provide detailed guidance on: the types of information/material to which overseers must have access; investigative powers, financial and human resources necessary to ensure such access and the appropriate use of information; and measures for protecting information handled by oversight (Open Society Foundations 2013: Principles 32, 33, 35). The Tshwane Principles also provide elaborate guidance on reporting and outreach by oversight bodies, including on the need for public versions of reports and mechanisms for ensuring public access to complaints procedure (Open Society Foundations 2013: Principle 34).

The Tshwane Principles are best known for their detailed recommendations on public access to information held by public authorities, including security services and their oversight bodies. The following guidelines are especially relevant for the purposes of informal oversight of security services by, for example, media organisations and NGOs.

- Public authorities must make information available on request, subject only to limited exceptions prescribed by law and necessary to prevent specific, identifiable harm to legitimate interests, including national security.
- No restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest.
- It is not sufficient for a public authority simply to assert that there is a risk of harm; the authority is under a duty to provide specific, substantive reasons to support its assertions.
- A person/organisation requesting information has the right to a speedy and low-cost review by an independent authority of a refusal to disclose information, or of matters related to the request. (Open Society Foundations 2013: Principles 1-5, 26)

Although the Tshwane Principles are the product of civil society they can be regarded as having significant weight in Europe because they have been endorsed through a PACE resolution and the European Parliament has also commended the principles.[57]

Ottawa Principles

The Ottawa Principles on Anti-terrorism and Human Rights were developed by a group of experts on human rights and counter-terrorism in 2006. These principles

57. PACE 2013: §§ 7-8; European Parliament 2014, § 77.

call for a pluralistic approach to the oversight of security services including internal controls within security services; the executive; an independent review body; legislative branch; judicial scrutiny; human rights, data protection freedom of information and audit institutions; and civil society (Ottawa Principles 2006: 9.1.1).

Especially useful is the enumeration in the Ottawa Principles of objectives for a system of oversight, which include ensuring the propriety; effectiveness; transparency; legitimacy and accountability of security service activities (Ottawa Principles 2006: 9.1.2).

The Ottawa Principles regard an independent review body (i.e. an expert non-parliamentary institution) as being at the heart of the system of oversight. They prescribe that such a body should, as a minimum, review propriety (legality) of security service activities and should also have a complaints-handling function (Ottawa Principles 2006: 9.3). In common with many other sets of recommendations, these principles also emphasise the need for overseers to have proper resources, access to information and investigative powers, and to issue public reports (Ottawa Principles 2006: 9.1.5, 9.3.3.b, d).

Necessary and Proportionate Principles

The 2013 *International Principles on the Application of Human Rights to Communications Surveillance*, drafted by leading privacy and security experts and endorsed by more than 400 NGOs and academic institutions, provide recommendations on the application of existing international legal standards to digital surveillance. A notable addition to the lexicon of international principles on the oversight of security services is the call for an independent oversight body to have the authority "to evaluate whether the state has been comprehensively and accurately publishing information about the use and scope of Communications Surveillance techniques and powers in accordance with its Transparency obligations … and to publish periodic reports and other information relevant to Communications Surveillance".[58] This recognises that oversight bodies have an important role to play in ensuring that security services become more transparent, which has implications for (re)developing public trust in security services.

58. https://en.necessaryandproportionate.org/text, Principle 10.

Chapter 4

NATIONAL PRACTICES IN COUNCIL OF EUROPE MEMBER STATES

Council of Europe member states have taken diverse approaches to structuring and undertaking oversight of their security services. This chapter will focus on national approaches to oversight by: (i) parliamentary committees; (ii) independent oversight institutions including expert security/intelligence oversight bodies and institutions with broader jurisdictions such as ombudspersons and data/information commissioners; and (iii) judicial bodies, including quasi-judicial bodies. To a lesser extent, the role of political executives and security services' internal control mechanisms will be considered. This chapter concludes by highlighting some examples of the role played by informal overseers: civil society and the media.

The handling of complaints relating to security services is dealt with in several chapters, reflecting the fact that Council of Europe states have vested these functions in a variety of oversight bodies. While ad hoc inquiries have played an important role in the oversight of security services, this paper deals only with standing oversight bodies, which exist on an ongoing basis. Rather than examining entire national oversight systems, examples are drawn from parts of various countries' systems. This is done with a view to highlighting contrasting approaches and good practices.

There is no Council of Europe member state whose system of oversight comports with all of the internationally or regionally recognised principles and good practices discussed in Chapter 5. Equally, it must be emphasised that there is no one best approach to organising a system of security service oversight. Diverse constitutional arrangements, legal and political systems, and historical contexts necessitate a range of approaches within the Council of Europe area. Accordingly, caution should be exercised when considering any wholesale importation or copying of examples from other states. There is, however, no doubt that there are models or practices that can be regarded as more effective for the purposes of safeguarding human rights in security service activity. These examples will be discussed in this chapter.

4.1 Parliamentary committees

Most Council of Europe member states have either established a parliamentary (sub) committee for overseeing security services (e.g. Italy, Germany and Poland) or given this function to a committee with a broader purview, such as home affairs, national security or defence (e.g. Georgia and Montenegro). Many parliamentary committees may also have legislative functions but this is beyond the scope of this issue paper.

Throughout the Council of Europe area there is a trend towards vesting parliamentary oversight of security services in a single committee that exists exclusively for the oversight of security services. Some states have created several oversight committees, each with responsibilities for a particular security service. For example, the Romanian parliament has separate oversight committees for its internal security service and foreign intelligence service, as well as a defence committee whose mandate includes some aspects of both services' work. This is also the case in Slovakia, which has separate committees for the oversight of the Slovak Information Service and for the National Security Authority. Such a division of labour may promote a greater level of specialisation and the accumulation of expertise among committee members. Conversely, the disadvantages of this approach include the risk that issues (such as information sharing between two security/intelligence services) may fall between the mandates of two or more committees (Venice Commission 2007: § 154) and that resources may be better concentrated on developing one committee.

Mandates and scope of oversight

In most Council of Europe states, the mandates of parliamentary oversight committees are loosely formulated, stipulating only that the committee exists to oversee/monitor/scrutinise given security services. For example, France's Délégation Parlementaire au Renseignement is tasked with overseeing "*l'activité générale et les moyens*" of various intelligence and security services. In Germany, the Parliamentary Control Panel is tasked with overseeing the "activities" of the security and intelligence services.[59] Most parliamentary oversight committees focus on a range of issues including the policy, finance and administration of services, as well as some aspects of completed operations (Wills and Vermeulen 2011: 92-95, 102-110, 115-116). Scrutinising compliance with the law is a pervasive matter that arises in all of these areas. However, some parliamentary committees, such as the Lithuanian Seimas Committee on Parliamentary Scrutiny of Intelligence Operations, have a specific mandate to examine security service compliance with constitutional rights and freedoms (in addition to other matters).[60]

Although the "depth" of oversight varies between parliamentary committees, the nature of these bodies means that most are not in a position to undertake regular, detailed oversight of operational activities including the collection, exchange and use of personal data. Such monitoring is increasingly undertaken by non-parliamentary

59. France 2007: Section 1.
60. Lithuania 2002: Article 23.

independent oversight bodies. This is primarily because this type of scrutiny is extremely time-consuming, highly specialised and resource intensive. For these reasons some Council of Europe states have chosen to supplement parliamentary oversight with more detailed, full-time scrutiny of operational activities and particularly the use and management of personal data (see below).

Regarding the temporal focus of oversight, European states' parliamentary committees perform almost exclusively *ex post facto* oversight, examining matters that have happened. There are no equivalents of the US practice of giving selected members of the congressional intelligence committees *ex ante* briefings on particular operations or programmes. From a human rights and accountability standpoint it is not desirable to involve oversight bodies *ex ante* given that they may then have to review such activities also *ex post* – there is an inherent risk of a conflict of interest arising.

Complaints handling

Some parliamentary oversight committees (e.g. in Poland, Hungary and Slovakia) are also charged with handling complaints against security services.[61] They are, however, unlikely to be able to provide an effective remedy as required under the ECHR because they cannot normally issue binding orders. Concerns may also arise as to whether political bodies are the most appropriate forums for impartially investigating complaints about violations of human rights. There is a clear risk that the handling of complaints could become politicised and that complainants would fail to obtain any redress due to attempts by governing parties to protect colleagues in the political executive.

Relationship with expert oversight bodies

Parliamentary oversight committees can also play an important role in monitoring the work of expert oversight bodies (see below); in other words, overseeing the overseers. This role can include: tasking expert oversight bodies to examine issues that parliamentary committees may not have the time, resources or expertise to examine;[62] evaluating their efficacy; appointing the members of these bodies; ensuring that they have the requisite powers and resources; holding hearings on their reports and giving effect (or pressing the executive to give effect) to recommendations made by these bodies. In Norway, for example, this role is performed by the Storting's Standing Committee on Scrutiny and Constitutional Affairs,[63] and in the Netherlands by the Intelligence and Security Committee of the second chamber, a special parliamentary committee composed of the chairpersons of political parties in the chamber (Verhoeven 2011: 254-255).

---

61. For further discussion see: Forcese 2012: 189-190.
62. For example, following the Snowden revelations, the Dutch parliament requested that the CTIVD Committee examine, *inter alia*, bulk collection by the Dutch services and any human rights implications: CTIVD 2014: 1.
63. For further discussion: Norway 2014: 5.

Access to classified information by parliamentary oversight committees

All parliamentary oversight committees have some access to classified information and in most cases the scope of their access is greater than that enjoyed by other members of parliament (Wills and Vermeulen 2011: 117-121). While the precise information needs of any oversight body are dictated by its mandate, it is good practice for parliamentary oversight committees to have access to all information that they deem relevant to the performance of their mandate and for restrictions (if any) to be as narrowly defined as possible. Romania's Joint Standing Committee on the Exercise of Parliamentary Control of the Romanian Intelligence Service (an internal security service) and Latvia's National Security Committee are examples of oversight committees that have unrestricted access to information.[64] Additionally, it is helpful for access to information by parliamentary oversight committees to be supported by proactive disclosure obligations for security services and/or the executive. Especially relevant for human rights protection are requirements to proactively disclose information on activities that have implications for the right to privacy. An excellent example in this regard is Germany, where the federal government must, every six months, disclose to the Bundestag's Control Panel a list including the implementation of surveillance measures, requests for information to private companies, Schengen alerts entered into the police information system and personal data sent to foreign entities.[65]

In some Council of Europe states there are concerns about parliamentarians, including members of parliamentary oversight committees, being given access to highly sensitive information and particularly information about security service operations. Such concerns are more common in post-authoritarian countries and those that have secessionist political parties represented in parliament. Various mechanisms have been devised to assuage such concerns, the most common of which is a requirement for prospective members of parliamentary oversight committees to be vetted and obtain a security clearance before taking their place on the committee.

This is a controversial practice for several reasons. First, security services may be required to vet their would-be overseers, which places the services (and thus the executive) in a position in which they have a *de facto* veto on the membership of parliamentary oversight committees. Such a position could be used to, for example, prevent a potentially critical member of parliament being appointed to an oversight committee. Second, there is a broader separation of powers issue that arises from the executive branch being able to influence or constrain the work of members of parliament, who have been selected by the electorate, through the security clearance process. Where vetting of MPs is required, it may be regarded as good practice for the vetting report produced by security services to be advisory only, with the final decision on the appointment of a parliamentarian to an oversight committee being

64. See Wills and Vermeulen 2011: 128-129. In the Romanian case there are restrictions on information on future and ongoing operations.

65. Germany 2001a: Section 14(1); Germany 1990b: Sections 8(a)(g), 17(3), 18(1)(a). See also: With and Kathmann 2011: 219-220.

taken by parliament. In Hungary, for example, it is parliament's National Security Committee that makes the final decision on whether a parliamentarian will take their place on the committee, notwithstanding the result of the vetting process (Földváry 2011: 231). Finally, vetting processes invariably require security services to seek highly sensitive personal data from and about members of parliament. Concerns may arise regarding how such information might later be used, particularly in situations where security services or the political executive are unhappy about the approach taken by a particular member of an oversight committee.

Alternatives to vetting have been adopted in various Council of Europe member states. Germany and Spain have adopted measures for the selection of members of parliamentary oversight committees that are designed to ensure that only parliamentarians who can command the support/trust of the legislature can be appointed and given access to classified information. In both countries a prospective member of the parliamentary oversight committee must receive the support of a qualified majority of the legislature in order to be appointed to the committee.[66] Having received such support there is no requirement for security clearance.

Other states have tried to address concerns about the protecting of information by requiring that parliamentary oversight committees can only access certain categories of classified information if they vote to do so by a qualified majority. For example, members of the Italian parliament's Committee for the Security of the Republic can vote by a two-thirds majority to lift any state secrecy privileges that would otherwise prevent their accessing operational information, when investigating the misconduct of intelligence officers (Italy 2007: Article 31(9)). Similarly, the Hungarian parliament's National Security Committee (whose members must also be security cleared) cannot ordinarily access the most sensitive information on operational methods but may vote by a two-thirds majority to lift this restriction in the context of a given investigation (Hungary 1995: Section 16(2)). Although such measures may prevent unreliable committee members fishing for information on their own, there is a real risk that governing parties could use their positions on oversight committees to block access to the most sensitive types of information and thus prevent activities from being investigated.

Advantages and disadvantages of parliamentary oversight

The main advantages of parliamentary oversight of security services can be summarised as follows. First, as elected representatives, overseers enjoy democratic legitimacy – scrutinising security services on behalf of those who elected them. Second, parliaments have recourse to legislative budget approval and sometimes to budgetary discharge powers, which can be used to ensure that the executive and the security services amend policies or practices that are not human rights compliant. Finally, parliamentarians are generally best placed to oversee the executive's role in directing and overseeing the security services. This is because in most Council of Europe states, parliament has a constitutional responsibility and right to hold the executive to account.

66. Sánchez Ferro 2011: 269; With and Kathmann 2011: 219.

There are also a variety of drawbacks associated with parliamentary oversight.[67] A primary weakness is that members of parliamentary committees have many competing demands on their time and may find it difficult to devote sufficient attention to the oversight of security services. This impacts upon the ability of parliamentary oversight committees to conduct the in-depth scrutiny of security service activity that is especially necessary for overseeing the legality of operational activity. A second and related feature of parliamentary oversight is that, in most cases, parliamentarians do not have any expertise on security services. This is exacerbated by competing demands on their time and, in many countries, short tenures of committee membership, thus preventing the accumulation of expertise. This weakness has been accentuated as security services have increased their usage of complex technology, which needs to be clearly understood in order for human rights implications to be fully assessed.

The most significant weakness of parliamentary oversight from the point of view of human rights protection is that effective scrutiny of security services may be undermined by the politicisation of oversight committees.[68] Parliamentarians are not always suited to the task of undertaking impartial scrutiny of security service compliance with the law. Party-political considerations may create incentives for parliamentary overseers to either protect security services and political executives from critical scrutiny or to undertake oversight with a view to causing political damage to opponents rather than ensuring the lawfulness (and effectiveness) of security service activity. Even where oversight committees are chaired by members of the opposition, governing parties can potentially use their majorities on oversight committees to limit scrutiny of aspects of security service activity that may be politically damaging. This is particularly problematic in countries where security services are still used and viewed as instruments of the political party/figure in government. Assessing compliance with the law is not an area of oversight suited to party politics and even the pursuit of political compromise on such committees can undermine effective human rights protection.[69]

Other relevant parliamentary committees

While this chapter has focused on oversight committees per se it should be noted that some states have established (sub) committees with niche mandates to oversee specific aspects of security service activity. Examples include the Spanish Cortes' Secret Funds Committee and the German Bundestag's Confidential Committee, both of which are responsible for scrutinising the budgets/finances of the security services.[70] Although this budgetary oversight may not appear to be directly concerned with human rights protection there is an important nexus because financial practices are often indicative of the broader propriety of programmes or operations. Activities that violate human rights often leave a financial footprint, the analysis of

67. See further: Wills and Vermeulen 2011: 88-89; and Farson 2012: 38-40.
68. See for example: Marty 2011: § 45.
69. Commissioner for Human Rights 2013a: §12; UNHCHR 2014: § 38.
70. See further: Wills 2012a: 163-164; Sánchez Ferro 2011: 271.

which can reveal information about such activities. Beyond these committees with niche mandates, many parliaments have other committees whose remits cover aspects of security service policy or activity. A good example is the work of the UK parliament's Joint Committee on Human Rights. The committee has, for example, considered security service policy within the context of broader thematic inquiries or legislative scrutiny on subjects such as counter-terrorism, the use of closed material procedures in courts and human rights obligations when dealing with foreign states with poor human rights records.[71] The main limitation on oversight by these "generic" committees is that in many cases they do not have the same rights of access to information as specialised oversight committees and they may also lack the security-specific expertise of oversight committees.

4.2 Independent oversight institutions

Expert security/intelligence oversight bodies

Expert oversight bodies are non-parliamentary entities that are set up specifically to oversee security services. Recognising the value of ongoing, expert, non-partisan oversight, an increasing number of Council of Europe member states have established expert security/intelligence oversight bodies. Such bodies are generally mandated to focus primarily on the legality of security service activity and policy, including on their compliance with human rights law. For example, this is the case in Norway the Netherlands and Portugal.[72] However, there are exceptions to this including Belgium's Standing Intelligence Agencies Review Committee (Committee I), which has a very broad mandate that also covers the effectiveness of security service activity and co-ordination between security services.[73] Unlike their parliamentary counterparts, expert oversight bodies focus primarily or exclusively on the security services themselves rather than on the executive's stewardship of these services.

In contrast to parliamentary oversight committees, expert bodies conduct their work on a (near) full-time basis. This generally means that they are able to provide more comprehensive and in-depth scrutiny than their parliamentary counterparts. Full-time, ongoing oversight is particularly important for monitoring the legality of security service work because this tends to be complex, time-intensive and detailed work. Where expert oversight bodies exist, they generally undertake the day-to-day scrutiny of security services and they are the mainstay of external oversight of security services in, for example, the Netherlands, Belgium, Croatia, Norway, Sweden and Portugal.[74]

---

71. See: www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/, accessed 28 March 2015.
72. Portugal 2004: Article 9(1); Norway 1995: s2; Netherlands 2002: Article 64(2).
73. Belgium 1991: Article 33; see also: http://comiteri.be/images/pdf/engels/w.toezicht%20-%20l.control.pdf; Committee I's website: http://comiteri.be/, both accessed 28 March 2015.
74. Portugal: www.cfsirp.pt/; for further information see: www.ennir.be/portugal/intelligence-review-portugal-0, both accessed 28 March 2015.

Membership

Expert oversight bodies' membership typically ranges from one to five and always includes people with legal/judicial expertise. In many cases members are former judges, former prosecutors and former politicians. These people are normally vetted and granted the highest level of security clearance. One of the important advantages offered by the expert oversight body approach is that overseers can (in theory although not always in practice) be selected on the basis of their expertise and experience. This is not usually the case with parliamentary oversight committees.

Statute or customary practice can dictate that the composition of the committee must include members with given experience or expertise. For example, in the Netherlands, the Review Committee on the Intelligence and Security Services (CTIVD) has developed a practice of including among its members a former senior law-enforcement official, alongside two members who must have legal expertise.[75] Recognising the political nature of some oversight activities and of intelligence work, some expert bodies such as Norway's EOS-Utvalget Committee include former parliamentarians and ministers alongside others with legal backgrounds. Croatia has adopted a particularly novel approach by requiring that its Council for Civilian Oversight of the Security and Intelligence Agencies include members who are academically qualified in political science, law and electro-technical sciences.[76] Past members of this body have included prominent members of civil society and human rights campaigners. Including people from diverse backgrounds in the oversight process ensures that competing and critical views are represented, which may in turn promote greater public confidence in oversight bodies.[77]

Expert bodies may be appointed by parliament (e.g. the Norwegian EOS-Utvalget Committee and the Council for the Oversight of the Intelligence System of the Portuguese Republic), the executive (e.g. UK Intelligence Services Commissioner and Sweden's Commission on Security and Integrity Protection) or a combination of the two (e.g. the Netherlands' CTIVD). Because members of expert oversight bodies are not sitting parliamentarians these institutions are sometimes viewed as lacking democratic legitimacy. To assuage such concerns and to reassure the public of the independence of expert oversight bodies from the executive, it may be prudent to involve parliament in the selection and appointment of their members. Such a link to the legislature can be further reinforced by their reporting directly to a given committee of parliament, as is the case in Belgium where the work of the Committee I is itself overseen by a committee of the chamber of representatives.

Scope of their work

Expert oversight bodies are typically mandated to scrutinise the lawfulness of security service activity including the collection and use of personal data by security services. A full assessment of human rights compliance requires scrutiny of:

- the authorisation of data collection;

75. CTIVD website: www.ctivd.nl/?English, accessed 28 March 2015.
76. Croatia 2006: Article 110(2); see further: Cvrtila 2012.
77. See for example comments by the former head of the UK's Secret Intelligence Service: (Norton-Taylor 2015).

- the collection process itself (including compliance with any warrant);
- any re-authorisation of measures;
- the retention, use and sharing of data by security services;
- requirements relating to the minimisation and/or deletion of data that have been obtained (particularly through untargeted surveillance); and
- the fulfilment of any requirement to notify persons of their having been subject to surveillance (where such requirements apply).

Examples of expert oversight bodies whose mandate covers this broad scope of security services' personal data-related activities include Germany's G10 Commission, the Netherlands' CTIVD and Sweden's Commission on Security and Integrity Protection (SIN).[78] By contrast, some expert oversight bodies have a narrower remit, focusing on selected aspects of data collection or use. For example, the UK's Interception of Communications Commissioner and the Intelligence Services Commissioner focus primarily on the authorisation process. Sweden's Defence Intelligence Inspection oversees the interception of international telecommunications and the quality and minimisation of data collected through these interceptions.[79]

Access to information and investigative powers

In various Council of Europe member states, the law requires that expert oversight bodies have full rights of access to information that they deem to be relevant to the fulfilment of their mandates, regardless of the provenance of such information.[80] Given the amount of information that is received from foreign bodies, it is essential that oversight bodies' access is not limited to information generated by the security services they oversee – meaning that they cannot view information of foreign provenance. Given that services collaborate more than ever with foreign partners and hold in their files an increasing amount of information supplied by foreign services, this would have the effect of shielding operations or areas of activity from independent scrutiny. Recognising this, several oversight bodies have made it clear that the third party rule (also called the principle of originator control) does not apply to them because they have legally guaranteed access to information held by the services/the executive that they oversee.[81]

Access to information may be supported by investigative powers including the power to subpoena individuals and documents and the right to inspect premises without notice. Although these powers are rarely used they reinforce the position of an oversight body when faced with a security service that is resistant to particular matters to be examined.[82] Belgium's Committee I even has a dedicated investigation service whose investigators can exercise police powers to secure the co-operation

78. Germany 2001a: Section 15(5); Cameron 2011: 280.
79. Bigo et al. 2013: 61; Cameron 2011: 281.
80. For example, UK 2000: Sections 58(1)(2) and 60(1); Netherlands 2002: Section 73(1); Norway 1995: Section 4.
81. For example: Norway 2014: 1; Laethem 2011: 199; Wills and Vermeulen 2011: 125.
82. Netherlands 2002: Article 74; Belgium 1991: Article 48(2); for a summary of investigative powers in selected European countries, see Wills and Vermeulen 2011: 134-135.

of security service officials (Belgium 1991: Articles 45, 49). Another powerful oversight tool is the right to access intelligence service systems and databases directly, generally through offices within security service premises. Norway's EOS-Utvalget Committee and the Netherlands' CTIVD both exercise this power.[83] This tool enables overseers to access and examine first-hand any files, systems or correspondence that is relevant to a given investigation, thereby making it more difficult for security services to hide anything from scrutiny. Such tools clearly have to be used diligently and only within the legal mandate of an oversight body.

An additional tool/power that has become especially essential is the right to call upon independent experts (who are security vetted) to advise on technical matters. As security and intelligence technology has become increasingly complex, a greater level of technical knowledge is required to understand and investigate systems used to collect, process and store information (including personal data). The human rights implications of such technology cannot be fully assessed without recourse to such expertise. Recognising the importance of this, some oversight bodies are empowered by law to hire technological experts to advise them on an ongoing basis.[84]

Complaints handling

Some Council of Europe states have mandated expert oversight bodies to handle complaints about security service activity including alleged unlawful surveillance and/or use of personal data. Examples include Belgium's Committee I, Sweden's SIN and Norway's EOS-Utvalget Committee. When compared with complaints handling by non-security-specific bodies, such as ombudspersons, this offers the advantage that the people handling complaints are likely to have broader contextual knowledge from their other oversight functions, which may assist in dealing with complaints. Such bodies also (should) have access to the most sensitive information, as well as the procedures and experience for handling it. This facilitates the expeditious handling of complaints and can, therefore, be a significant advantage as compared to more general venues for complaints handling, such as ombudspersons (Forcese 2012: 186). From the point of view of human rights protection, it is notable that expert oversight bodies do not generally have the power to make legally binding determinations following the investigation of a complaint. Generally, they can only make recommendations and representations to services and the political executive, rather than being able to order the payment or compensation or deletion/correction of personal data.[85] For example, in Sweden the SIN may make a finding that, for instance, a complainant's personal data were not processed in accordance with the law. However, the SIN would then need to refer the person to the chancellor of justice who decides whether compensation should be paid and, if necessary, it would need to refer the matter to the data protection authority to order the deletion of personal data (Cameron 2011: 284).

83. Verhoeven 2011: 257; Norway 2014: 5.
84. Norway 2012, Norway 2013 and Norway 2014; see also: With and Kathmann 2011: 221; Cameron 2011.
85. For a discussion of this issue, see: Forcese 2012: 192-193; Hernes 2008: 81-82.

Making non-binding recommendations is not sufficient to provide a complainant with an effective remedy. A requirement to delete or correct personal data and/or pay compensation is the most common and necessary remedy in relation to personal data collection and use by security services. Given that most expert oversight bodies cannot make binding decisions, it remains necessary for people whose rights have been violated by security services to have parallel or subsequent access to some form of body that can provide such remedies. When considering whether an effective remedy is available, a system of oversight can be looked at in the round.

Ombudspersons

The mandates of ombudspersons vary significantly across Europe and most do not play a significant role with regards to the oversight of security services. In many countries the possibility exists for an ombudsman to investigate complaints about the security services but they rarely do so in practice. Ombudspersons can, however, play a valuable role by both handling complaints relating to security services and undertaking own-initiative investigations into security services. This is particularly true in states that do not have expert security/intelligence oversight bodies or strong parliamentary oversight committees.

A notable example of an ombudsperson that plays an active role in the oversight of security services is the Serbian Protector of Citizens. This office investigates complaints relating to the security services, takes a proactive role in launching own-initiative investigations of security service activity and has successfully challenged security service laws in the constitutional court.[86] Serbia has demonstrated that empowering ombudspersons to challenge laws that are not constitutional is useful for protecting human rights. An ombudsperson is likely to be much better placed than individuals or NGOs to bring such challenges. The ombudsman of the Netherlands also handles complaints about the security and intelligence services but complainants may only approach the ombudsman after having raised a complaint with the relevant ministry and been dissatisfied with the response received.

In common with many expert security/intelligence oversight bodies, one of the drawbacks to the ombudsperson model is that most of these institutions may only issue recommendations. This is not sufficient in cases in which human rights have been violated and a person is due an effective remedy.

Data protection authorities (DPAs) and information commissions

DPAs and information commissions are independent oversight bodies responsible for scrutinising compliance by public bodies (and in some cases private bodies) with data protection legislation and/or freedom of access to information legislation. These functions are often performed by a single body.

86. See for example: Protector of Citizens of the Republic of Serbia 2010; Protector of Citizens of the Republic of Serbia 2014: 14-15, 207-211.

The extent to which DPAs oversee security services' use of personal data depends on whether data protection legislation covers security services, whether a DPA's mandate extends to the security services, limitations on people's right to access personal data held by security services and any restrictions on a DPA's access to classified information. A recent study by the EU's Article 29 Working Group found that there are very few European countries where DPAs conduct full supervision of the use of personal data by security services and that they are often excluded entirely from this domain. Nevertheless, a number of these institutions have a mandate and actively oversee security service use of personal data and/or requests to access information held by security services (Article 29 2014a: §§ 9-10).

A DPA's role may include scrutinising the handling of and decisions on individual requests for access to personal data held by security services. They may also conduct their own-initiative investigations and inspections on the handling/processing of data by security services. For example, Germany's Federal Data Protection Commissioner examines security services' compliance with data protection law, with the exception of data collected through surveillance (which is dealt with by another body, the G10 Commission), and its biennial reports cover these matters (With and Kathmann 2011: 227). The Slovenian and Serbian information commissions play a similar supervisory role.[87]

In many European countries security services are entirely exempt from freedom of information/access to information legislation (Jacobsen 2013: 9-10). This means that members of the public cannot apply to access particular documents and information commissioners have no powers to recommend or require that information be disclosed. Switzerland is an example of a country where the security service is not exempt from the law on the freedom of information. The Federal Administrative Tribunal confirmed recently, in a case brought by a journalist seeking access to the summaries of reports produced by the intelligence service, that even information that is classified is potentially disclosable.[88] The Federal Data Protection and Information Commissioner oversees the handling of requests for information by the public. This is also the case in Slovenia where the Information Commissioner scrutinises security service reasoning for non-disclosure of information and may order the declassification of information in appropriate circumstances (Jacobsen 2012: 17).

Finally, both the Slovenian and Serbian information commissioners have also used their positions to challenge data retention and surveillance legislation before their respective constitutional courts. These are excellent examples of the capacity of independent oversight bodies to provide checks not only on the human rights compliance of practices of security services but also the legal framework that underpins these services.

4.3 Judicial bodies

Although the courts may scrutinise and adjudicate on the action and output of security services in many contexts, this section will focus on the role of judicial bodies in

87. Slovenian Information Commissioner: www.ip-rs.si/?id=195, accessed 28 March 2015; Serbian Information Commissioner: www.poverenik.rs/index.php, accessed 28 March 2015; see also: Petrović 2012: 21-23.

88. Stoll 2014; Goumaz 2014.

authorising intrusive surveillance measures by security services and in adjudicating on complaints arising from (alleged) security service activity.

Complaints against security services

Regarding claims against security services, most Council of Europe states offer the theoretical possibility of an individual bringing an action to seek a remedy. Bringing an action may be more straightforward when a person wishes to challenge an arrest, interrogation or detention (in the few countries that permit security services to exercise such powers). However, as mentioned above (see section 2.4 on the right to a fair trial), there are often significant obstacles to litigating against security services. Using the courts to challenge security service surveillance or data use is even more complex because, in most cases, an individual will not find out about such infringements of their rights (Venice Commission 2007: § 243). Challenges are only likely to be brought if an individual finds out about such measures through some form of notification requirement, by accident, from a whistleblower or through some other legal proceedings. There are sometimes explicit restrictions on persons seeking to challenge secret surveillance in ordinary courts before they have been notified of their having been targeted (Germany 2001a: Section 13).

The UK has created a special judicial body, the Investigatory Powers Tribunal (IPT), for handling complaints about surveillance and all human rights-related claims against the security services.[89] It has exclusive jurisdiction to adjudicate on such claims. Such a model has the advantage that it can investigate challenges to (alleged) surveillance even while that surveillance may be ongoing and it can make binding orders in the event that measures are found to be unlawful. In 2015, the Tribunal handed down its first ruling against the security and intelligence services, finding that aspects of international intelligence sharing violated Articles 8 and 10 of the European Convention on Human Rights because they were not in "accordance with the law".[90] In spite of this success, there are significant drawbacks to this tribunal model and it has been heavily criticised.[91] Notably, complainants may not be informed about hearings, they have no automatic right to be present during hearings or represented by a lawyer of their choice, no reasons may be given for a decision and the IPT's decisions are not appealable or amenable to judicial review.

Authorisation of intrusive measures

The majority of Council of Europe member states require their security services to obtain judicial warrants in order to use measures for collecting information that are deemed to be particularly intrusive with regards to the right to privacy and family life. Exceptions to exclusively judicial models of authorisation include the UK and the Netherlands (executive authorisation), Poland (approval of a judge and an independent prosecutor general who is not part of the executive) (Poland

89. UK 2000: Sections 65-67; for the IPT's website, see: www.ipt-uk.com/, accessed 28 March 2015.
90. *Liberty & Others vs. the Security Service, SIS, GCHQ.*
91. See for example: JUSTICE 2011: 133-153; Leigh 2012: 438-439.

2002: Article 27), Belgium and Germany (forms of quasi-judicial authorisation), and Romania (authorisation by special prosecutors).[92]

Although the types of measures requiring external authorisation vary, they commonly include the targeted interception of communications (where the person/organisation whose communications are to be intercepted is known at the outset), search and seizure of property and the installation of recording devices in dwellings. By contrast, in most states judicial authorisation is not, for example, required for information collection using human sources, untargeted bulk surveillance, computer network exploitation, searching pre-existing data banks gathered through bulk surveillance, obtaining data gathered by other government departments and accessing data held by private companies. A notable exception is Serbia where the security service must now obtain judicial authorisation not only for secret surveillance or recording of any form of communications but also for obtaining communications data and for conducting searches of data that have already been acquired through the use of intrusive powers (Serbia 2014: Articles 13 and 15). This approach is a useful example in view of the ongoing debates about better controlling security service access to data that have been gathered through bulk collection, for example, as well as access to communications data.

The Snowden revelations have raised questions about the extent of judicial authorisation of untargeted bulk surveillance of either cable-bound or non-cable-bound communications. While there is limited information in the public domain on this subject, the laws of most Council of Europe member states do not explicitly require judicial authorisation of such measures (to the extent they are permitted by national law and within the capabilities of a security service). However, Sweden has a special court for authorising untargeted bulk interception of cable- and non-cable-bound international communications (i.e. those that are not deemed to be exclusively domestic). Made up of two judges plus six lay judges, the Defence Intelligence Court grants warrants to the Defence Radio Establishment (FRA) to use particular selectors/search streams on specific international cables.[93]

While the precise modalities of the application and consideration of judicial warrants differ between states, in most cases the role is performed by a single senior judge who is specially designated either in law or selected through a process prescribed by law. For example, in Bosnia and Herzegovina, the relevant judge is the president of the court of Bosnia and Herzegovina or a judge designated by him/her. In Hungary it is a judge appointed by the president of the metropolitan court and in the Czech Republic the relevant judge is chair of the panel of high court judges in the relevant geographical region.[94] Croatia provides an additional safeguard for the re-authorisation/prolongation of the intrusive measures, which must be done by a panel of three judges rather than the single judge for the initial authorisation (Croatia 2006: Articles 36 and 37(2)).

92. Romania 1991: Article 13. Note the Court's criticisms of this approach to authorisation as not fully independent of the executive: *Dumitru Popescu v. Romania* [69-73].
93. Cameron 2011: 281; Bigo et al. 2013: 61; Pond 2013.
94. Bosnia and Herzegovina 2004: Article 77; Hungary 1995: Section 58; Czech Republic 1994 § 9(1).

Generally, judges make authorisation decisions on the basis of paper applications but some countries provide for application hearings where complex issues arise or a judge wishes to ask questions of a security service representative. Proceedings are necessarily *ex parte* and in most states the would-be subject of intrusive measures is not represented in any way. Norway has adopted a novel approach whereby the interests of the would-be target of surveillance measures by the security police are represented by a security-cleared lawyer who has the opportunity to challenge the basis for the warrant put forward by the security service.[95] This is done through written submissions. Sweden's Defence Intelligence Court (see above) is said to use a similar system as part of the authorisation of warrants to intercept international communications (Pond 2013). Beyond Europe, the US President's Review Group on Intelligence and Communications Technologies called for the creation of a public interest advocate "to represent the interests of those whose rights of privacy or civil liberties might be at stake".[96] Including such a person in the process of authorising intrusive measures offers better human rights protection because it enables the authorising body to hear competing views, including on the interpretation of points of law, and it helps to ensure that the justifications put forward by security services are subject to critical analysis.

Judicial authorisation is often regarded as offering the best safeguards for human rights. This is primarily because judges are generally regarded as independent, impartial and unlikely to be swayed by political considerations surrounding security service activity, which might influence a minister making authorisation decisions. Judges are also regarded as being better suited to assessing legal criteria such as necessity and proportionality, which is clearly important when the measures sought may have significant human rights implications.

Judicial authorisation is not, however, a panacea that guarantees respect for human rights in the authorisation and use of intrusive measures by security services (Venice Commission 2012: § 35). There are a number of potential drawbacks to judicial authorisation. First, the efficacy of judicial authorisation as a human rights safeguard depends to a large extent on the independence of the judges concerned. In countries where judges are not independent it is unlikely that they will take a particularly critical approach to requests from security services to use intrusive measures. Second, expertise is similarly integral to the efficacy of judicial authorisation (Venice Commission 2007: §§ 205-206). Judges with limited experience (and even those with experience) of security matters may be highly reluctant to second-guess the national security assessments of a security service official applying for a warrant (Cameron 2008: 45). This is sometimes compounded by the tendency of some judges to be highly deferential to the executive on matters of national security. Third, concerns have also been expressed that in many jurisdictions judicial authorisation amounts to rubber-stamping decisions taken by security services, with very few requests for warrants being turned down (UNHCHR 2014: § 38). Finally, and closely linked to the problem of rubber-stamping, is the fact that judges cannot normally be held to account for the warrants they issue to security services. In order to preserve judicial

95. Norway 1981: Section 100a; Norway 2014: 8.

96. Review Group on Intelligence and Communications Technologies 2013: 203-204 and Recommendation 28.

independence and the separation of powers, warrant-issuing processes are not usually subject to *ex post* scrutiny by an oversight body (Cameron 2011: 285). By contrast, a minister or quasi-judicial authorising body can more easily be held to account in parliament or by an independent oversight body for the decisions it makes and this possibility may have a salutary effect on decision making (Borger 2014).

4.4. Quasi-judicial authorisation bodies

In the Council of Europe area there are several states where intrusive measures must be authorised by a quasi-judicial body. Belgium has recently adopted a novel approach to the authorisation (and oversight) of the use of certain intrusive measures. An administrative commission (SIM Commission)[97] comprised of three security-cleared magistrates (acting in a non-judicial capacity) appointed by the executive, gives "binding advice" to the security services when they apply to use "exceptional measures" (i.e. the most intrusive of three categories of measures).[98] These exceptional measures include observation in and searches of private dwellings; hacking into electronic systems; the interception of communications; and the use of human agents including through the creation of false identities. It is unusual for human intelligence operations, such as use of informants or the infiltration of organisations, to require authorisation by an independent body and in this regard Belgian law gives recognition to the human rights implications of human intelligence operations. More significantly, Belgian law recognises the human rights implications of hacking/CNE and requires that such measures be authorised by an external body. There is a second category of less intrusive "specific measures" (including the identification of the user of a communications service and accessing electronic communications data) that can be authorised by the head of the relevant security service. However, they must first notify the SIM Commission and the services must also report on the use of such measures on a monthly basis.[99]

Belgium's complex system for the authorisation of intrusive measures also provides for the ongoing oversight of the use of measures authorised by the SIM Commission in order to assess their legality (specifically including their proportionality). The Commission has the power to suspend the use of intrusive measures or, in the case of less intrusive measures the service director has authorised, it can order that any data collected cannot be used. For its part, the SIM Commission must inform an expert oversight body (Committee I – see above) of authorisations and extensions granted or refused. Committee I examines all of the authorisations and the implementation of the measures by the security services. This expert oversight body is empowered to effectively overrule the SIM Commission's decisions to approve, refuse or suspend measures.[100] This oversight of the authorisation body provides an additional human rights safeguard.

97. Its full title is: La commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité.
98. Belgium 2010: Articles 18 (2)(3)(9)(10), 43(1).
99. Belgium 1998: Articles 18 (2) (3).
100. For a detailed insight into Committee I scrutiny of these measures, see: Belgian Standing Intelligence Agencies Review Committee 2012: 143-169; Belgium 1998: Articles 43(3) (3)(4)(5).

The German approach to the authorisation of intrusive measures also merits consideration. Such measures must in the first instance be authorised by a designated government minister who then applies to an institution called the G10 Commission for authorisation (which can in some instances be retroactive). This applies not only to targeted surveillance but also to untargeted surveillance using selectors or search terms, the legality (including proportionality) of which the G10 Commission evaluates. With regards to untargeted surveillance, the G10 Commission also scrutinises the minimisation of data obtained through surveillance.[101] Appointed by the parliamentary oversight committee, the G10 Commission can be viewed as quasi-judicial since it is chaired by a person who is qualified to hold judicial office (but who is not acting in a judicial capacity); the other three members may or may not be members of the Bundestag.[102]

Requiring the authorisation of both a member of the executive and independent decision makers, including judges[103] or a quasi-judicial body, offers significant advantages from a human rights point of view. It ensures that there is a double "check" beyond a security service and potentially ensures that the qualities of both executive and judicial authorisation are built into the process.

4.5. Executive

The political executive is a customer, taskmaster, controller and overseer of security services. It cannot be regarded as a genuinely external overseer because executive departments are part of the security intelligence process – they task, authorise, set policies and priorities for security services (Venice Commission 2007: § 129). In all Council of Europe member states there is one or more members of the executive responsible for security services. Generally, security services fall under broader ministerial portfolios such as defence, justice, interior or home affairs but they may also fall under the prime minister (e.g. in Turkey), a president (e.g. in Romania) or under the joint authority of a president and prime minister (e.g. in Croatia). Executive control and oversight may also be exercised by a collective body such as a national security council, as is the case in Croatia and Serbia. In Croatia for instance, the National Security Council is supported by the Office of the National Security Council, which is responsible for, among other things, monitoring the legality of security service activities (Croatia 2006: Article 107(1)). This is in addition to the oversight of legality provided by an external expert oversight body (see above).

Executive responsibilities also include formulating directives, subsidiary regulations, general policies and priorities for security services. These functions include issuing guidance on how human rights must be taken into account and ensuring that policies and priorities accord proper weight to human rights considerations. For example, the UK government has issued guidance to its security and intelligence services on

101. Germany 2001a: Section 10(1); With and Kathmann 2011: 221-223; Venice Commission 2015: §§ 124-125.

102. Germany 2001a: Section 15.

103. Canada is an example of a non-Council of Europe state which also uses a two-layered approach to authorisation, including a deputy minister and federal court judge. See: Canada 1984: § 21(1).

sharing intelligence in relation to persons who are in the custody of/being questioned by foreign security services (UK 2010). The executive is in a prime position to ensure that security services conduct their work in compliance with human rights. In view of this, external oversight bodies can seek to ensure that ministers exercise their powers to, for instance, formulate codes of ethics or regulations on information sharing with foreign partners.

Lastly, in several Council of Europe member states ministers are also responsible for authorising the use of surveillance measures[104] and authorising key words/search terms that can be used by security services when searching so-called communications data (Bigo et al. 2013: 74). Where ministers do play such a role, it is essential that they have access to advisers who can help them to assess the human rights and broader legal implications of any proposed measures.

4.6. Internal controls

While this issue paper focuses on external oversight, security service managers and their staff play the leading role in ensuring that their activities are lawful and comply with human rights. It is individual members of security services, not external overseers, who are present when many decisions with important human rights implications are made. For this reason, the values, ethics and legal knowledge of security service personnel is of utmost importance. With this in mind, security service managers have to implement robust selection vetting criteria to ensure that they only recruit people with appropriate values. They also need to ensure that ongoing training is provided, including on human rights issues (Venice Commission 2007: § 132) and on the role played by external oversight bodies. It is essential that external oversight bodies scrutinise these internal policies and practices of security services.

Ultimately, effective systems of external oversight count for little if security services are not committed to undertaking their work with respect for human rights and in a manner that facilitates oversight and accountability (Venice Commission 2007: §§ 130, 134). Equally, if external oversight is to be effective in promoting human rights compliance and accountability within security services there needs to be a willingness to collaborate with oversight bodies and to take on board their recommendations.

All security services put in place internal procedures for the authorisation of particular measures, the review of their activities, the proper recording of activities and the reporting of any concerns.[105] In most cases these procedures are put in place by senior management, but they may also be required by law. For example, in Germany the security services are required to ensure that surveillance measures are implemented under the supervision of a member of staff who is qualified to hold judicial office.[106] Some Council of Europe member states, such as Italy, Bosnia and Herzegovina and Serbia, have also legislated to create inspectors-general within security services. The

104. For example: UK 2000: Sections 7 and 8; Netherlands 2002: Article 19 (with the exception of post, which must be authorised by a court, per Article 23).
105. For an overview see: Born and Leigh 2005: 46-49.
106. Germany 2001a: Section 11(1).

functions of these internal inspectors include assessing the lawfulness of service activity.[107] Although this oversight function can be useful for alerting service managers and the executive to any problems, internal inspectors-general are not a substitute for robust external scrutiny.

4.7. Media and civil society

The role of the media in covering security issues varies greatly within the Council of Europe area and depends, *inter alia*, on media ownership, laws protecting journalists' sources and the human and financial resources of media organisations. The media has often been ahead of the official oversight "curve", uncovering and investigating issues such as rendition and secret detention before standing oversight bodies (Priest 2005). In many cases the work of journalists has precipitated inquiries by standing and ad hoc oversight bodies.

Journalists play a particularly important role in uncovering unlawful security service activity in contexts in which official systems of oversight are either failing to detect or failing to address practices that violate human rights (PACE 2011: § 8). They may also be an outlet for members of security services who are seeking to bring to light concerns about illegality but who are unable to get concerns addressed through prescribed channels, have no confidence in such channels or where no authorised external channel for making disclosures exists.

Non-governmental organisations (NGOs) also play a role in monitoring and publicising the work of oversight bodies. NGOs in the Western Balkans have been especially active in this regard and there are a number of NGOs that specialise in rule of law issues in the security sector. By way of example, since the adoption of the Law on Parliamentary Oversight of the Security and Defence Sector in 2010, Montenegro's Institut Alternativa has conducted annual studies on the implementation of the law, focusing primarily on the performance of the committee charged with oversight of the security sector.[108] It is important that NGOs (and the media) focus not only on the security services but also on the institutions that oversee them.

NGOs also play an important role in bringing and intervening in litigation relating to security services before the Court and national courts. Organisations such as the Open Society Justice Initiative, Reprieve and the Polish Helsinki Foundation for Human Rights played a role in bringing human rights claims arising from the involvement of European states in US-led secret detention and rendition activities. Several NGOs, including Privacy International, Big Brother Watch and Liberty have played an instrumental role in bringing domestic and international litigation against governments in relation to surveillance laws and practices. *Liberty and Others v. the United Kingdom* (in which the Strasbourg Court found the UK's previous legal framework for bulk collection of international communications to be incompatible with the Convention) is but one example. The contribution of NGOs remains vital in the context of ongoing challenges to bulk surveillance measures, international intelligence sharing and CNE by security services.

---

107. Bosnia and Herzegovina 2004: Article 33(1); Petrović 2012: 14-15.

108. See: http://institut-alternativa.org/?lang=en, accessed 28 March 2015.

NGOs can also assist by campaigning for inquiries on security service activity and contributing their expertise to such inquiries, as well as making submissions when parliament is adopting or amending laws governing security services. These organisations have drawn attention to perceived flaws in oversight and accountability processes and campaigned for more robust, independent ad hoc inquiries into security service activity over the past decade (Townsend 2014).

The ability of the media and NGOs to provide informal oversight of security services depends to a great extent on there being an environment in place in which they can challenge governments on sensitive matters without fear of harassment or retribution. This is not the case in a number of Council of Europe member states. The existence and scope of freedom of information laws also affects the ability of the media and NGOs to work on these issues. While many Council of Europe member states have placed security services outside the ambit of these laws, some national laws enable persons/groups to request information from or about security services and require services to justify (under external supervision) decisions not to disclose information. Such approaches to freedom of information enable civil society organisations and media to obtain information that can assist their work without posing a risk to national security.

Chapter 5

TOWARDS DEMOCRATIC AND EFFECTIVE OVERSIGHT OF NATIONAL SECURITY SERVICES

It is evident from the international principles and national practices discussed in this paper that oversight systems can be constituted in many different ways while pursuing similar objectives. When designing and evaluating oversight systems, it is helpful to focus on substance rather than on the form of the oversight. This allows for common objectives to be pursued while making allowances for different constitutional and legal set-ups, as well as different national traditions. The purpose of this final chapter is to highlight a number of the important principles and objectives that emerge from the foregoing analysis.

An overarching principle that can be drawn from the international principles and state practices discussed above is that all aspects of security service activity, policy, finance, administration and regulation should be subject to scrutiny by at least one institution that is external to and independent from the security services and the executive. International principles and the practices of many Council of Europe member states demonstrate that this external scrutiny should be *ex ante* (where appropriate), contemporaneous and *ex post*.

The broad objectives of oversight systems must include holding security services and (where relevant) the political executive to account for and helping to promote:

- the efficacy of security services in fulfilling their legal mandates, including their role in helping to forestall threats to human rights posed by, for example, terrorism, espionage and cybercrime;
- the efficiency, financial propriety and value for money of security services; and
- the legality and human rights compliance of regulations, policies and operations.

The third of these objectives has been the focus of this issue paper and is the overriding objective underpinning the other objectives discussed in this chapter. It is worth reiterating that although this issue paper has focused on external oversight of security services, internal checks and controls within these services are fundamentally important for fulfilling the aforementioned objectives.

Democratic oversight is important because security services (and related executive departments) provide a public service to and on behalf of the public and therefore elected representatives must be involved in ensuring that this service is provided effectively, efficiently and lawfully. Accordingly, the "democratic" aspect of oversight is primarily achieved through the involvement of parliament. Experience from Council of Europe member states demonstrates that parliamentarians should contribute by: ensuring that national laws provide for comprehensive oversight of security services; allocating the necessary budgetary resources to non-parliamentary oversight institutions; overseeing the work of expert oversight bodies; keeping under review the efficacy of oversight institutions (including their own committees); and conducting both ongoing scrutiny and ad hoc inquiries into security service activity.

Parliamentary oversight of security services remains essential in any democracy but there is growing recognition, as shown by international principles and state practice, that human rights and the rule of law are best protected when oversight by parliamentarians is supplemented by expert oversight. Expert oversight bodies are generally better placed to undertake the ongoing, detailed and politically neutral scrutiny that human rights protection requires. This type of oversight is particularly necessary with regards to the scrutiny of security service activities that impact upon the rights to privacy, freedom of expression, assembly and association. Such activities include the collection, use, storage, transfer (including to domestic law-enforcement agencies and foreign bodies) and deletion of personal data. As expert oversight bodies play a growing role in the oversight of security services it is important to ensure that steps are taken to ensure that these institutions have some democratic legitimacy. Accordingly, various Council of Europe member states have parliamentary committees that monitor the work of expert overseers, appoint (and remove) members and receive their reports.

5.1. *Ex ante* authorisation of intrusive measures

Regarding the *ex ante* authorisation of intelligence collection, human rights are best protected when a body that is independent from the security services and political executive is required to authorise intrusive measures. There is growing support for the view that external authorisation should extend to:

- untargeted bulk collection of information;
- the use of key words or selectors to extract data from the information collected through bulk interception, particularly where they are related to identifiable individuals;
- the collection of and access to communications data (including when held by the private sector);
- computer network exploitation.

As has been discussed, the human rights implications of these activities are too significant to be authorised by the executive alone or (worse) auto-authorised by security services. External authorisation of these measures should be done by a judicial or quasi-judicial body, or through a combination of one these bodies and the executive.

Including different types of expertise in the process of authorising intrusive measures may provide stronger safeguards than authorisation by a body that is either political or judicial. An authorisation process undoubtedly needs to encompass legal and human rights assessments of proposed measures but it may also be beneficial to address any political risks associated with proposed measures. Accordingly, a two-level authorisation process combining authorisation by a (quasi-)judicial body with that of a minister may offer the most robust model of *ex ante* scrutiny.

As with any part of the intelligence collection process, the process by which intrusive measures are authorised or re-authorised should itself be subject to scrutiny. Given the difficulties that may arise when seeking to evaluate judicial decisions on the authorisation of intrusive measures, consideration may be given to quasi-judicial models. Quasi-judicial authorisation, which has become more common in the Council of Europe area, incorporates judicial expertise without giving the authorising body judicial status. As state practice shows, the work of such bodies can be scrutinised by another oversight body without giving rise to the concerns associated with potential *ex post* scrutiny of judicial decisions.

The protection of human rights through authorisation processes can also be improved through the inclusion of advocates to represent the interests of would-be targets (and in the case of bulk surveillance the collateral victims) of surveillance and potentially other forms of intrusive measure such as CNE. This third party can challenge security service proposals for surveillance and their involvement reduces the risk that authorisation processes simply become rubber-stamping exercises.

5.2. Complaints handling

All Council of Europe member states are required to ensure that their oversight systems include a designated independent body to which complaints about security services can be made. Regardless of whether this is an expert security/intelligence oversight body or non-security-specific oversight body such as an ombudsperson, complaints must be handled by a body that has the requisite access and investigative powers to conduct thorough investigations. Most oversight bodies can only issue recommendations to security services and/or the executive. Given that the ECHR requires that persons who believe (or know) that their rights have been unlawfully infringed by security services must have access to an institution that can provide an effective remedy, states must ensure that individuals can also access an institution equipped to make legally binding orders. The powers of such a body should include not only granting compensation to the victims of any violations but also the power to quash relevant warrants and order the deletion of personal data that have been collected unlawfully.

5.3. Access to information by overseers

Access to information by overseers is of paramount importance and is referred to in almost all international principles relating to oversight. Overseers cannot make complete or reliable assessments of, *inter alia*, the legality of operations, programmes

and policies unless they have access to all of the information concerned. While it is not an end in itself, access to all information relevant to an investigation (and the broader mandate of a given oversight body) is a pre-condition for effective scrutiny. The right of oversight bodies to access information should be accompanied by a duty for security services and their personnel to be open and co-operative with their overseers as well as requirements that given categories of information should be disclosed automatically. Recourse to investigative powers, such as subpoenas and search and seizure, further reinforces the position of overseers in cases where information is not willingly provided.

Granting overseers access to information does not mean that oversight bodies should have unlimited access to any information at all times – the basis for access must always be the mandate and current activities of a given oversight body.

Given that it is clearly established as best practice for at least one external oversight body to be mandated to oversee each area of security service activity, it follows that at least one external overseer should have unrestricted access to information relating to each area. Accordingly, an essential objective when designing and improving oversight systems is to ensure that access to information by overseers is legally guaranteed and supported by appropriate investigative tools to facilitate such access. A fundamental principle for effective oversight is that oversight bodies (not security services or the executive, who are the subjects of scrutiny) should determine what information is relevant to their work. If there are disputes in this regard mechanisms should exist to resolve them expeditiously.

A necessary corollary of ensuring that overseers have access to all relevant information is the need to implement measures for ensuring that information handled by overseers is protected and used only for the purposes of oversight. As long as oversight bodies have procedures in place to ensure that sensitive information is not misused, there is no good reason why their members should be trusted any less than members of the executive branch or security services.

Access to information arising from and pertaining to international intelligence co-operation merits special consideration. In view of the extensive international co-operation between security services (and the impact that such co-operation can have on human rights) it is essential that overseers are able to scrutinise information about such co-operation, including information that has been received from or sent to foreign bodies. Ensuring that overseers are not regarded as "third parties" or subject to the principle of originator control either in law or in practice is essential for ensuring proper scrutiny of these activities. Democratic oversight is seriously undermined when foreign bodies have an effective veto (by virtue of security services having to request the permission of foreign partners before their overseers can view information) on what an oversight body can scrutinise.

A further objective is to ensure that overseers have access to the necessary financial and human resources to enable them to be effective. Many security services have growing capacities (by virtue of technological changes and increased budgets) to collect, share and receive information and use increasingly complex systems for doing so. Most overseers have not seen increases in their resources to match these developments. It is now widely recognised that recourse to independent technical

expertise has become indispensable for effective oversight. Intelligence collection and storage systems have become more complex and their human rights implications cannot easily be assessed without recourse to specialist expertise. Laws should therefore permit overseers to hire technical experts and resources must be provided to enable them to do so.

5.4. Transparency of oversight bodies

Oversight bodies scrutinise security services on behalf of the population. Important objectives in this regard are providing assurance (where warranted) to the public that security services are performing their functions in accordance with the law and reporting (where appropriate) on things that have been done wrong. Oversight bodies can only do this if they demonstrate through their reporting and other forms of outreach that security services are subject to robust oversight and that any instances of human rights violations (or other wrongdoing) are addressed. A secondary objective in this regard is to educate the public about the role of security services in a democracy. This is especially important for societies in which security services have in the past violated human rights and/or are not trusted by the public. With these objectives in mind, it is essential that parliamentary and expert oversight bodies engage with the public to the greatest extent possible. They should be required to publish public versions of their periodic and special/ad hoc reports, taking appropriate account of the need to keep certain details confidential for reasons of national security and privacy.

5.5. Evaluation of oversight systems

Considerable progress has been made in the Council of Europe area on establishing external oversight of security services but very few countries have gone on to undertake reviews of the efficacy of individual oversight bodies, let alone oversight systems.[109] Having legislated to establish oversight bodies, in many cases 10 to 20 years ago, most states have not revisited these arrangements or have only done so following significant scandals or intelligence failures. Consequently it is very difficult to know whether oversight systems, for example: focus on the most relevant aspects of security service activity; are effective in helping to improve the human rights compliance of security service policies, operations and regulations; use effective methods and conduct sufficiently demanding investigations; have the confidence of the public; or provide accurate and useful reports.

As discussed above, for oversight systems to be effective in preventing and responding to human rights concerns in/arising from the work of security services they require an appropriate legal mandate and powers, resources and expertise. Such requirements

109. Exceptions include Belgium and the Netherlands: Sénat et Chambre des Représentants de Belgique, "Evaluation du fonctionnement des Comités permanents de contrôle des services de police et de renseignements", Rapport fait au nom des commissions spéciales chargées du suivi parlementaire des comités permanents de contrôle des services de police de renseignements par MM. Foret and De Crem, 16 février 1996. 437/1 – 95/96 Chambre, 1-258/1 Sénat; Fijnaut 2012.

evolve as the nature, scale and technology used in security service work evolves. Accordingly, it is essential that oversight systems be periodically evaluated to assess whether or not they do possess the necessary attributes.

A related consideration is whether – notwithstanding the adequacy of their legal mandates, powers and resources – oversight bodies (and oversight systems more broadly) can be regarded as performing their functions effectively. This includes considering whether they are efficacious in ensuring that security service policies, operations and practices promote and comply with human rights, as well as whether complaints are handled and responded to in a way that promotes both redress and institutional improvements. Evaluating such matters necessitates in-depth analysis of the work of overseers' methods and approaches. Consequently, before undertaking official evaluations, there is a need to consider how the effectiveness of oversight can be evaluated and, in particular, how the capacity of an oversight system to protect human rights could be assessed.[110] These are matters for further debate and potential work on a European level.

Parliaments and ministers can play an important role in this regard by ensuring evaluation clauses are built into legislation governing security services and their oversight.[111] Alternatively, the executive, parliament or oversight bodies can set up such evaluations on an ad hoc basis, as was done recently in the Netherlands. An alternative or supplementary model has been adopted in the UK, which has created an Independent Reviewer of Terrorism Legislation.[112] Although this office focuses on counter-terrorism legislation more broadly, the incumbent is addressing the adequacy of legislative provisions relating to oversight and is empowered to make recommendations in this regard.

110. For further discussion see: Wills 2012b: 471-499.

111. The best example in this regard comes from outside the Council of Europe area: Canada 1984: § 56; Canada 1990.

112. See: https://terrorismlegislationreviewer.independent.gov.uk/, accessed 28 March 2015.

References

Article 29 Working Party (2014a), Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN WP 215, 10 April 2014.

Article 29 Working Party (2014b), Joint Statement of the Article 29 Working Party, adopted 26 November 2014.

Balkan Insight (2015a), "Serbian ombudsman complains of threats", 21 January 2015: www.balkaninsight.com/en/article/serbian-ombudsman-threaten-after-military-secret-service-revelation, accessed 28 March 2015.

Balkan Insight (2015b), "Macedonia PM accused of large-scale wire-tapping", 9 February 2015: www.balkaninsight.com/en/article/eavesdropping-bombshell-explodes-in-macedonia, accessed 28 March 2015.

BBC News (2015), "Sim card firm links GCHQ and NSA to hack attacks", 25 February 2015: www.bbc.co.uk/news/technology-31619907, accessed 28 March 2015.

Belgian Standing Intelligence Agencies Review Committee (2011), *Annual report 2010-2011*, Intersentia, Brussels. Available at: www.comiteri.be/images/pdf/publicaties/activity_report_2010-2011.pdf, accessed 28 March 2015.

Belgium (1991), Act governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment 1991. Available at: http://comiteri.be/images/pdf/engels/w.toezicht%20-%20l.control.pdf, accessed 28 March 2015.

Belgium (1998), Law on the Intelligence and Security Services 1998.

Belgium (2010), Law on the Intelligence and Security Services 1998, (as modified by the law on collection of data by the intelligence and security services of 14 February 2010).

Bigo D. et al. (2013), "National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law", European Parliament, Brussels.

Bigo D. et al. (2014), "France's surveillance: justice, freedom and security in the EU", openDemocracy.net, 14 May 2014.

Borger J. (2013), "NSA files: why the Guardian in London destroyed hard drives of leaked files", *The Guardian,* 20 August 2013.

Borger J. (2014), "Ministers should assess UK surveillance warrants, says Philip Hammond", *The Guardian,* 23 October 2014.

Born H. and Leigh I. (2005), *Making intelligence accountable*, Parliament of Norway, Oslo.

Born H., Leigh I. and Wills A. (forthcoming), *Making international intelligence cooperation accountable*, Parliament of Norway, Oslo.

Bosnia and Herzegovina (2004), Law on the intelligence and security agency of Bosnia and Herzegovina 2004.

Cameron I. (2000), *National security and the European Convention on Human Rights*, Martinus Nijhoff Publishers, The Hague.

Cameron I. (2008), "National Security and the European Convention on Human Rights – Trends and Patterns", speech to the Stockholm International Symposium on National Security and the European Convention on Human Rights, 4-5 December 2008.

Cameron I. (2011), "Parliamentary and specialised oversight of security and intelligence agencies in Sweden", in Wills A. and Vermeulen M. (eds) (2011), "Parliamentary oversight of security and intelligence agencies in the European Union", European Parliament, Brussels.

Cameron I. (2013), "Foreseeability and safeguards in the area of security: some comments on ECHR case law", in *Regards sur le contrôle*, Laethem W. (Van) and Vanderborght J. (eds) (2013), Intersentia, Antwerp.

Canada (1984), Canadian Security Intelligence Service Act 1984.

Canada (1990), "In flux but not in crisis", Canada Special Committee on the Review of the CSIS Act and the Security Act (NCJ 131163), Ottawa, Canada.

Cobain I. (2013), *Cruel Britannia: a secret history of torture,* Portobello Books, London.

Commissioner for Human Rights, Council of Europe (2013a), "Human rights and the security sector: report of the round-table with human rights defenders, organised by the Office of the Council of Europe Commissioner for Human Rights, Kyiv, 30-31 May (2013)", CommDH(2013)17.

Commissioner for Human Rights, Council of Europe (2013b), "Human rights at risk when secret surveillance spreads", Human Rights Comment, 24 October 2013.

Commissioner for Human Rights, Council of Europe (2014a), *The rule of law on the internet and in the wider digital world,* Issue Paper, Council of Europe, Strasbourg.

Commissioner for Human Rights, Council of Europe (2014b), Statement of 12 December 2014: www.facebook.com/permalink.php?story_fbid=377981239044459&id=118705514972034, accessed 28 March 2015.

Commissioner for Human Rights, Council of Europe (2014c), "Report by Nils Muižnieks, Council of Europe Commissioner for Human Rights, following his visit to the Netherlands, from 20 to 22 May 2014", CommDH(2014)18, 14 October 2014.

Commissioner for Human Rights, Council of Europe (2015), "4th quarterly activity report 2014", CommDH(2015)3.

Connolly K. (2014), "Romanian ex-spy chief acknowledges CIA had 'black prisons' in country", *The Guardian,* 14 December 2014.

Council of Europe (2006a), "Secretary General's report under Article 52 ECHR on the question of secret detention and transport of detainees suspected of terrorist acts, notably by or at the instigation of foreign agencies", SG/Inf (2006)5, 28 February 2006.

Council of Europe (2006b), "Secretary General's supplementary report", SG/Inf (2006)13, 14 June 2006.

Croatia (2006), Act on the Security Intelligence System of the Republic of Croatia, 30 June 2006.

CTIVD (2014), "Review report on the processing of telecommunications data by GISS and DISS", No. 38, 5 February 2014.

Cvrtila V. (2012), "Intelligence governance in Croatia", DCAF. Available at: www.dcaf.ch/content/download/104961/1617969/version/2/file/croatia_eng1.pdf, accessed 28 March 2015.

Czech Republic (1994), Act on the Security Information Service, Act No. 154 of July 7, 1994.

European Data Protection Authorities (2014), Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, adopted 26 November 2014, 14/EN WP227.

European Parliament (2001), "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)", Temporary Committee on the ECHELON Interception System, 11 July 2001, A5-0264/2001.

European Parliament (2007), "Resolution on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners", 14 February 2007, P6_TA(2007)0032.

European Parliament (2013), "Resolution of 10 October 2013 on alleged transportation and illegal detention of prisoners in European countries by the CIA", P7_TA(2013)0418.

European Parliament (2014), "Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs", A7-0139/2014, 21 February 2014.

Farson S. (2012), "Establishing effective intelligence oversight systems" in Born H. and Wills A. (eds) (2012) *Overseeing intelligence service: a toolkit,* DCAF, Geneva.

Fijnaut C. (2012), "Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel, De vertrekpunten en uitkomsten van een gespreksronde", The Hague.

Földváry G. (2011), "Parliamentary and specialised oversight of security and intelligence agencies in Hungary", Annex A in Wills A. and Vermeulen M. (2011), *Parliamentary oversight of security agencies in the European Union*, European Parliament, Brussels.

Follorou J. (2014), "Espionnage : comment Orange et les services secrets coopèrent", *Le Monde*, 20 March 2014.

Follorou J. and Johannès F. (2013), "Révélations sur le Big Brother français", *Le Monde,* 4 July 2013.

Forcese C. (2012), "Handling complaints about intelligence services", in Born H. and Wills A. (eds), *Overseeing intelligence services: a toolkit*, DCAF, Geneva.

France (2007), Loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement.

Gallagher R. and Greenwald G. (2014), "How the NSA plans to infect 'millions' of computers with malware", *The Intercept,* 3 December 2014: https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/, accessed 28 March 2015.

Germany (2001a), Act restricting the Privacy of Correspondence, Posts and Telecommunications (G10 Act), *Federal Law Gazette* I, p. 1254, revised 2298, last amended by Article 2 of the Act of June 6 2013, *Federal Law Gazette* I, p. 1482.

Germany (1990b), Act on the Protection of the Constitution (BVerfSchG), *Federal Law Gazette* I, p. 2954, last amended by Article 6 of the Act of June 6, 2013, *Federal Law Gazette* I, p. 1602.

Germany (1978), Parliamentary Control Panel Act (PKGrG), *Federal Law Gazette* I, p. 453, last amended by the Act of July 29, 2009, *Federal Law Gazette* I, p. 2346.

Goumaz M. (2014), "Statut spécial voulu par les espions", *Le Temps,* 1 July 2014.

Hernes H. (2008), "Effective Remedy with Regard to Secret Surveillance and Security Files", speech to the Stockholm International Symposium on National Security and the European Convention Human Rights, 4-5 December 2008.

Higgins A. (2013), "Luxembourg's prime minister resigns", *New York Times,* 12 July 2013.

Human Rights Watch (2009), *Cruel Britannia, British complicity in the torture and ill-treatment of terror suspects in Pakistan,* November 2009.

Human Rights Watch (2014a), *Rights in retreat: abuses in Crimea,* Human Rights Watch, New York.

Human Rights Watch (2014b), "Turkey: spy agency law opens door to abuse", April 2014: www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse, accessed 28 March 2014.

Hungary (1995), Act CXXV of 1995 on the National Security Services, section 16(2).

International Commission of Jurists (2009), *Assessing damage, urging action: report of the Eminent Jurists Panel on terrorism, counter-terrorism and human rights*, ICJ, Geneva.

Italy (2007), Law 127/2007 (as amended 1 August 2012).

Jacobsen A. (2012), "Regional consultation on national security and the right to information", www.right2info.org/resources/publications/national-security-page/european-questionnaires/slovenia-rosana-lemut-strle, accessed 28 March 2015.

Jacobsen A. (2013), "National security and the right to information in Europe", April 2013: www.right2info.org/resources/publications/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe, accessed 28 March 2015.

JUSTICE (2011), *Freedom from suspicion: surveillance reform for a digital age*, Justice, London.

Laethem W. (Van) (2011), "Parliamentary and specialised oversight of security and intelligence agencies in Belgium", in Wills A. and Vermeulen M. (2011), "Parliamentary oversight of security and intelligence agencies in the European Union", European Parliament, Brussels.

LAHRC (2015), Draft Resolution adopted by LAHRC on 26 January 2015.

Le Monde (2013), "La DCRI accusée d'avoir illégalement forcé la suppression d'un article de Wikipédia", 6 April 2013.

Leigh I. (2012), "A view from across the Channel: intelligence oversight in the UK", in Laethem W. (Van) and Vanderborght J. (2012) (eds), *Regards sur le contrôle*, Intersertia, Antwerp.

Lithuania (2002), Law on Operational Activities 2002 (as amended).

Marty D. (2011), "Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations", Report for the Committee on Legal Affairs and Human Rights, Doc. 12714, 16 September 2011.

Nemtsova A. (2012), "Putin's secret war," *Foreign Policy,* June 2012.

Netherlands (2002), Intelligence and Security Services Act 2002. Available at: www.ctivd.nl/?download=WIV%202002%20Engels.pdf, accessed 28 March 2015.

Norton-Taylor R. (2015), "Britain needs independent scrutiny of intelligence, says former head of MI6", *The Guardian,* 17 March 2015.

Norway (1981), Criminal Procedure Act, Act of 22 May 1981 No. 25 (as amended).

Norway (1995), Act relating to the Oversight of Intelligence, Surveillance and Security Services Act No. 7 of 3 February 1995. Available at: http://eos-utvalget.no/english_1/legal_framework/content_3/text_1401199215164/1401199215664/lovengelsk.pdf, accessed 28 March 2015.

Norway (2012), EOS-Utvalget Committee, *Annual Report 2011*.

Norway (2013), EOS-Utvalget Committee, *Annual Report 2012*.

Norway (2014), EOS-Utvalget Committee, *Annual Report 2013*.

Omtzigt, P. (2015), "Mass surveillance", PACE Committee on Legal Affairs and Human Rights, 26 January 2015, [AS/Jur (2015) 01].

Open Society Foundations (2013), Global Principles on National Security and the Right to Information (Tshwane Principles), adopted on 12 June 2013 in Tshwane, South Africa: www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf, accessed 28 March 2015.

Open Society Justice Initiative (2013), *Globalizing torture: CIA secret detention and extraordinary rendition,* OSF, New York.

Osborne L. (2013), "Germany denies phone data sent to NSA used in drone attacks", *The Guardian,* 12 August 2013.

Ottawa Principles on Anti-terrorism and Human Rights, adopted in 2006 in Ottawa, Canada: http://aix1.uottawa.ca/~cforcese/hrat/principles.pdf, accessed 28 March 2015.

PACE (2005), Parliamentary Assembly of the Council of Europe Recommendation 1713 (2005), 23 June 2005.

PACE (2011), Parliamentary Assembly of the Council of Europe Resolution 1838 (2011), 6 October 2011.

PACE (2013), Parliamentary Assembly of the Council of Europe Resolution 1954 (2013), 2 October 2013.

Petrović P. (2012), "Serbia", Strengthening intelligence oversight in the Western Balkans series, DCAF, Geneva. Available at: www.dcaf.ch/content/download/104944/1617879/version/2/file/serbia_eng1.pdf, accessed 28 March 2015.

Poland (2002), Act of 24 May 2002. Internal Security Agency and Foreign Intelligence Agency.

Pond E. (2013), "What the NSA can learn from Sweden", World Policy Blog, 9 August 2013, www.worldpolicy.org/blog/2013/08/09/what-nsa-can-learn-sweden, accessed 28 March 2015.

Portugal (2004), Intelligence Systems of the Portuguese Republic, Framework Law 4/2004.

Priest D. (2005), "CIA holds suspects in secret prisons", *Washington Post*, 2 November 2005.

Privacy International (2014), Statement of Grounds submitted to the Investigatory Powers Tribunal, 8 May 2014: www.privacyinternational.org/sites/default/files/PI%20Hacking%20Case%20Grounds.pdf, accessed 28 March 2015.

Protector of Citizens of the Republic of Serbia (2010), "Report on a preventive control visit by the Protector of Citizens to the Security-Information Agency", (Belgrade, 2010). Available at: www.ombudsman.org.rs/attachments/088_Report%20on%20the%20Preventive%20Control%20Visit.pdf, accessed 28 March 2015.

Protector of Citizens of the Republic of Serbia (2014), Annual Report for 2013. Available at: www.ombudsman.rs/attachments/2013%20Annual%20Report%20of%20the%20Protector%20of%20Citizens.pdf, accessed 28 March 2015.

Review Group on Intelligence and Communications Technologies (2013), "Liberty and security in a changing world", 13 December 2013: www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, accessed 28 March 2015.

Romania (1991), Law on the National Security of Romania, No. 51/July 29 1991.

Sánchez Ferro S. (2011), "Parliamentary and specialised oversight of security and intelligence agencies in spain", Annex A in Wills A. and Vermeulen M. (2011), "*Parliamentary oversight of security agencies in the European Union*", European Parliament, Brussels.

Serbia (2014), The Law on Security Information Agency Official Gazette of the Republic of Serbia (as amended in 2014), Official Gazette Nos. 42/2002, 111/2009, 65/2014 – US, 66/2014.

Singh A. and Scholes J. (2014), "Denmark, the CIA, and the killing of Anwar al-Awlaki", 30 April 2014: www.opensocietyfoundations.org/voices/denmark-cia-and-killing-anwar-al-awlaki, accessed 28 March 2015.

Stark H. (2011), "Germany limits information exchange with US intelligence", *Der Spiegel,* 17 May 2011.

Stoll M. (2014), "Des documents du SRC peuvent aussi être publics", Oeffentlichkeitsgesetz.ch, 15 December 2014: www.oeffentlichkeitsgesetz.ch/francais/2014/12/des-documents-du-src-peuvent-aussi-etre-publics/#more-3569, accessed 28 March 2015.

Townsend M. (2014), "UK rights groups reject official inquiry into post-September 11 rendition", *The Observer,* 8 November 2014.

Travis A. and Bowcott O. (2015), "UK admits unlawfully monitoring legally privileged communications", *The Guardian,* 18 February 2015.

Turkey (2014), Law Amending the Law on State Intelligence Services and the National Intelligence Agency, No. 6532, April 2014.

UK (2000), Regulation of Investigatory Powers Act (RIPA) 2000.

UK (2010), "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", Cabinet Office, London, July 2010.

UN (1987), UN Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 10 December 1984 (entry into force 26 June 1987).

UN (2010a), "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", Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 17 May 2010, A/HRC/14/46.

UN (2010b), "Joint study on global practices in relation to secret detention in the context of countering terrorism", Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/13/42, 19 February 2010.

UN (2013), "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue", 17 April 2013, A/HRC/23/40.

UN (2014), "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.

UN General Assembly (2013), Resolution 68/167, 18 December 2013, A/RES/68/167.

UN General Assembly (2014), Resolution 69/166, A/RES/69/166, 18 December 2014.

UN Human Rights Committee (2004), "General Comment Number 31", UN Doc. CCPR/C/21/Rev.1/Add.13 (2004).

UN Human Rights Council (2009), Resolution 10/15, 10th Session, 26 March 2009.

UNHCHR (2014), "The right to privacy in the digital age", 30 June 2014, A/HRC/27/37, UN High Commissioner for Human Rights. Available at: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf, accessed 28 March 2015.

Venice Commission (1998), "Internal security services in Europe", 7 March 1998, CDL-INF (98) 6.

Venice Commission (2007), "Report on the democratic oversight of the security services", 11 June 2007, CDL-AD(2007)016.

Venice Commission (2012), "Revised draft opinion on the federal law on the Federal Security Service (FSB) of the Russian Federation", Opinion no. 661/2011.

Venice Commission (2015), "Update of the 2007 Report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies", adopted at the 102nd plenary session (Venice, 20-21 March 2015, CDL-AD(2015)006.

Verhoeven N. (2011), "Parliamentary and specialised oversight of security and intelligence agencies in Germany", in Wills A. and Vermeulen M. (2011), "Parliamentary oversight of security agencies in the European Union", European Parliament, Brussels.

Wills A. (2012a), "Financial oversight of intelligence services," in Born H. and Wills A. (eds) (2012), *Overseeing intelligence services: a toolkit,* DCAF, Geneva.

Wills A. (2012b), "Who's watching the overseers? Ad hoc evaluations of intelligence oversight and control bodies", in Laethem W. (Van) and Vanderborght J. (eds), *Regards sur le contrôle*, Intersertia, Antwerp.

Wills A. and Vermeulen M. (2011), "Parliamentary oversight of security and intelligence agencies in the European Union", European Parliament, Brussels.

With H. (De) and Kathmann E. (2011), "Parliamentary and specialised oversight of security and intelligence agencies in Germany", in Wills A. and Vermeulen M. (2011), "Parliamentary oversight of security agencies in the European Union", European Parliament, Brussels.

Court cases

European Court of Human Rights

Abu Zubaydah v. Lithuania, Application No. 46454/11, communicated on 14 December 2012.

Al Nashiri v. Poland, Application No. 28761/11, 24 July 2014.

Al Nashiri v. Romania, Application No. 33234/12, communicated on 18 September 2012.

Assenov and Others v. Bulgaria, Application No. 90/1997/874/1086, 28 October 1998.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application No. 62540/00, 28 June 2007.

Big Brother Watch and Others v. the United Kingdom, Application No. 58170/13, lodged on 4 September 2013 (challenging PRISM and TEMPORA).

Dumitru Popescu v. Romania, Application No. 71525/01, 26 April 2007.

El Masri v. "the former Yugoslav Republic of Macedonia", Application No. 39630/09, 13 December 2012.

Husayn (Abu Zubaydah) v. Poland, Application No. 7511/13, 24 July 2014.

Iordachi and Others v. Moldova, Application No. 25198/02, 10 February 2009.

Kennedy v. the United Kingdom, Application No. 26839/05, 18 May 2010.

Klass and Others v. Germany, Application No. 5029/71, 6 September 1978.

Leander v. Sweden, Application No. 9248/81, 26 March 1987.

Liberty and Others v. the United Kingdom, Application No. 58243/00, 1 July 2008.

Malone v. the United Kingdom, Application No. 8691/79, 2 August 1984.

Nasr and Ghali v. Italy, Application No. 44883/09, communicated on 22 November 2011.

Segerstedt-Wiberg and Others v. Sweden, Application No. 62332/00, 6 June 2006.

Sunday Times v. the United Kingdom (No. 2), Application No. 13166/87, 26 November 1991.

Vetter v. France, Application No. 59842/00, 31 May 2005.

Weber and Saravia v. Germany, Application No. 54934/00, decision on admissibility of 29 June 2006.

National courts

Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, Joined Cases C-293/12 and C-594/12, 14 April 2014.

Liberty & Others vs. the Security Service, SIS, GCHQ, IPT/13/77/H, 6 February 2015.

Disclosures by US intelligence contractor Edward Snowden about bulk surveillance of electronic communications have given rise to serious concerns about violations of the right to privacy and family life, freedom of expression and freedom of association. These ongoing revelations follow a decade of others on the involvement of some security services in serious human rights violations. All of this brings into question the adequacy of the legal regulation and oversight of security service activity in the Council of Europe area.

This issue paper focuses on the role of national institutions responsible for authorising, monitoring, scrutinising and reviewing security service activity and, to a lesser extent, executive bodies responsible for security services. The following types of oversight institution are considered through examples from various European states: parliamentary committees, judicial and quasi-judicial bodies, expert security and intelligence oversight bodies, data and information commissioners, ombudsman institutions and the executive and internal control mechanisms within security services.

Alongside analysis of national oversight practices, this issue paper also takes stock of the growing body of international hard and soft law principles relevant to the supervision of security services. Particular attention is paid to the relevance of the European Convention on Human Rights and its case law in this area. The publication gives special emphasis to the oversight of activities that generate ongoing human rights concerns, including co-operation with security and intelligence services of other states, untargeted, bulk surveillance of electronic communications and computer network exploitation (hacking).

The issue paper sets out a series of recommendations on how the supervision of security services can be enhanced to promote better protection of human rights in this area of state activity. Recognising that there is no single "best" model or system of oversight, the recommendations put forward principles that can be implemented in any political or constitutional set-up.

www.commissioner.coe.int

PREMS 050415

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, 28 of which are members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE