DCAF Parliamentary Brief

Safeguards in Electronic Surveillance

Why is this topic important for Members of Parliament?

Who uses electronic surveillance and why?

What safeguards should be put in place to prevent the misuse of electronic surveillance?

1. ***Comprehensive legislation***
2. ***Control mechanisms***
3. ***Effective oversight***

What is the role of Parliament in the oversight of electronic surveillance?

What other resources are available on safeguards in electronic surveillance?

DCAF

a centre for security, development and the rule of law

This Parliamentary Brief provides practitioners with a concise introduction into the main concepts, principles and good practices in building safeguards that prevent the misuse and abuse of intrusive methods of information collection – with a focus on electronic communications surveillance.

Why is this topic important for Members of Parliament?

Electronic surveillance is used across European countries to fight serious crime, terrorism, and avert dangers to state security. It is a covert, intrusive method for information collection, performed in secrecy and without the knowledge of the target; it requires security services to possess special, exceptional powers, which often infringe fundamental human rights, primarily the right to privacy.

Therefore, electronic surveillance is a field where abuse is potentially easy in individual cases, but can inflict harmful consequences for the democratic society as a whole, undermining public trust in the state.

Box 1. Terminology and types of surveillance

Audio Surveillance includes phone-tapping, voice over internet protocol (VOIP), and listening devices (room bugging).

Data Surveillance includes computer/internet (spyware/cookies), blackberries/mobile phones and keystroke monitoring.

Electronic Surveillance includes audio surveillance, visual surveillance, tracking surveillance, and data surveillance.

Focused Surveillance is the monitoring, whether electronic or physical, of a specific individual or group of individuals based on a prior suspicion of a threat to security.

Mass Surveillance is the monitoring of a large fraction or entirety of a population by intercepting and filtering through electronic communications, searching for key words and phrases to detect possible security threats.

Metadata is data that describes other data - such as geographic origination of communication or the time stamp on a communication.

Tracking Surveillance includes global positioning systems, radio frequency identification devices, and biometric information technology.

Visual Surveillance includes hidden video surveillance devices, in-car video systems, body worn devices, thermal imaging, forward looking infrared, and CCTV.

The use of electronic surveillance is not a new phenomenon; however the scale and the purpose of electronic surveillance today create controversy. Technological progress enables access to a much larger volume of data than in the past and platforms for data extraction have multiplied. Moreover, the distinction between targeted electronic surveillance for criminal investigation purposes and large scale surveillance for national security objectives becomes increasingly blurred. These trends in electronic surveillance pose a high risk of abuse, arbitrariness and misuse.

The extensive use of electronic communication surveillance by intelligence agencies has been brought to the forefront public scrutiny in recent years, after the disclosures made by Edward Snowden, a former US national security insider. The surveillance practices developed by the USA and their allies endanger fundamental human rights, including the right to privacy (Art. 8 of the European Convention for Human Rights - ECHR), freedom of information and expression (Art. 10), and the rights to a fair trial (Art. 6) and freedom of religion (Art. 9). These rights are cornerstones of democracy. Their infringement without adequate judicial control and parliamentary oversight jeopardize the rule of law.

Legislation of communications surveillance differs across states, but often, it is characterised by ambiguity or loopholes, while national oversight bodies lack the capacity to effectively monitor the lawfulness of both targeted and large scale interception of data. Regulatory questions concerning intrusive methods of investigation have only recently started to be addressed in European Union countries, as issues related to data protection are challenged by courts, law makers and the public at large.

In April 2014, the European Court of Justice declared invalid the 2006 Data Retention Directive, which instructed EU governments and telecommunications companies to save individuals' data and communications records for a minimum of six months, in the interest of national investigatory measures. The Court found that the Directive violated rights prescribed by the EU Charter of Fundamental Rights: the right to private life guaranteed by Art. 7, and the protection of personal data guaranteed by Art. 8. The wide-ranging and particularly serious interference of the Directive with the fundamental rights in question was deemed to be insufficiently circumscribed to ensure limitation to what is strictly necessary.

Box 2. Intrusive methods of information collection

Tap, receive, record and monitor conversations, telecommunication, other data transfer or movement – within the country or from abroad.

Conduct surveillance, record, and trace information.

Conduct search of enclosed spaces, intrusion into property.

Open letters and other consignments, without consent of the sender or addresser.

Request providers of public telecommunication networks to furnish information relating to identity of users and the traffic taking place.

Use stolen or false identities, keys, software for clandestine entering, copying or corrupting databases.

Have access to all places for installing observation.

Collect financial information on individuals or networks.

Reports, studies, opinions and working documents are plentiful, indicating that national and EU regulations are in the midst of a reform process that will set limits to the scale of surveillance and search for more meaningful oversight.

However, one democratic imperative is already underscored by all EU institutions: legal safeguards must be instituted by parliaments, allowing security and intelligence agencies to conduct information collection while protecting citizens' rights. Ensuring the fundamental balance between national security and human rights requires countries to undertake comprehensive assessments of electronic surveillance laws and practices. Analysis should not be reduced to the question of data protection versus national security. Instead, it must be framed in terms of collective freedoms and democratic principles.

Who uses electronic surveillance and why?

Both intelligence and police agencies utilize intrusive methods for information collection. However, the purpose and the level of authorisation for their use, is significantly different.

Intelligence services use intrusive methods to detect and monitor threats to national security, prevent and disrupt acts of terror or aggression, whether internal or external. A proper definition of what *national security*

actually means is lacking across a majority of EU members states. How states define national security, threats to national security and the measures security services can employ in order to address these threats is a matter of national sovereignty, therefore significant differences may appear between different legal regimes. A common denominator for most countries is that national security has moved away from a one-dimensional Cold War approach, related to the "*threat of war by a foreign enemy*", to include today broad and changing notions like criminal activities, terrorism or migration.

Intelligence services are often the main users of **strategic** or **mass surveillance** techniques, meaning that they record large volumes of electronic communication about *unknown threats*. They receive records from telecommunications companies and use government mass filtering computer programs. Much of the information obtained with mass surveillance technics is **metadata** – describing basically the time and the geographic location of communication, but not its content. Metadata collection has sparked controversies across the world as to whether or not it constitutes a violation of privacy and how to best regulate it.

Police services use intrusive methods for information collection in order to gather evidence about suspected criminal activity: detect culpability in an impending crime or prove a prior crime already committed by a suspect.

Police are the main users of **focused surveillance**, targeted on *known threats*: a specific individual or group of individuals and a specific type of communication. Procedures for the collection of targeted information are usually subject to clear, detailed authorisation and renewal process, including a maximum period the data collection can take place. Law enforcement agencies are sometimes able to access metadata to assess the composition of criminal networks. The electronic surveillance practices of law enforcement agencies are often authorised by a different, or lower ranking government institution and judicial court.

A big difference between the intelligence and police in utilizing intrusive methods is that information collected by law enforcement is used as evidence in courts – which determine the admissibility of evidence and therefore decide if the methods were used in agreement with laws and constitutional rights. In contrast, information collected by intelligence agencies is rarely used in court trials. Collection justified by *national security* purposes often produces information which is classified. UK and Netherlands are among the few EU countries allowing for the formal use of classified information in judicial proceedings. But in a majority of countries, secret evidence is not legal evidence, as it is considered that the rights of the defence and the right to a fair trial cannot be "*balanced*" against national security or states interests. Therefore, the way intrusive methods for information collection are implemented by intelligence agencies is not subject to ex-post judicial control. This, combined with the legal uncertainties inherent to the term "*national security*", allow for a disproportionate margin of appreciation by state authorities in cases of strategic surveillance.

Besides intelligence and police services, the legal authority to use intrusive powers for information collection may be granted to border and tax authorities, military intelligence, or prosecuting agencies who investigate serious crime, terrorism or anticorruption. However, not all these agencies might possess technical capacities for electronic surveillance; therefore the implementation of intrusive methods may be outsourced to relevant agencies who own this capacity. Therefore, for a comprehensive assessment of the use of intrusive methods for information collection in a country, all agencies that possess the legal authority and/or the technical capacity to implement such measures must be carefully identified and classified.

What questions could a Member of Parliament ask to assess a country's use of intrusive methods?

- Which state agencies are authorised to use intrusive methods for information collection?
- Which state agencies have the technical infrastructure to implement intrusive methods?
- How many surveillance measures were executed within one year? How many of these measures were executed for national security purposes and how many were executed for criminal investigations? How many of these measures had resulted in indictments, and subsequently in condemnations?
- What is the relationship between state agencies and telecommunications/internet service providers?
- Do laws clearly state the details of surveillance measures, responding to the questions: what, when, how and by whom?

What safeguards should be put in place to prevent the misuse of electronic surveillance?

In order to set limits in the use of intrusive methods for information collection, there should be three main safeguards put in place:

1. Comprehensive legislation,
2. Control mechanisms (executive and judicial),
3. Effective oversight.

1. Comprehensive Legislation

The legal basis regulating the use of intrusive methods of information collection should be drafted considering the following **crucial principles**:

Necessity and subsidiarity: Intrusive methods should only be implemented as a method of last resort, meaning that they should be considered only after less intrusive means have proven ineffective or when there is no reasonable alternative to obtain crucial information or evidence.

Proportionality: The intrusion into privacy should be proportionate to the seriousness of the suspected offence and the evidence that is anticipated to be obtained. There must also be both a respect for human rights, and at the same time, an awareness of the dangers posed by the suspected offense.

Detailed instruction: If legislation on the use of intrusive methods is vague and unspecific, undemocratic means of authorisation will always become a practice, filling in legislative gaps. Therefore, the legal base must be clear, publicly accessible and specifying:

- The nature of offences that give rise to the use of such methods (relevant crimes must be defined according to specific criteria);
- The category of persons liable to be subject to intrusive methods;
- The duration of surveillance/interception;
- Strict procedures to be followed for examining, using and storing the data obtained;
- Precautions and limitations to be taken when communicating the data to third parties;
- The circumstances and procedures for data destruction;
- Precautions to be taken to protect privileged communication (i.e. between attorney and client);
- The bodies responsible for supervising the use of surveillance powers (which should be independent; responsible to and appointed by the Parliament rather than the Executive).

Box 3. Swiss legislation on the use of intrusive methods

Switzerland's 2011 **Criminal Procedure Law 312 – Chapter 8** sets forth specific requirements that must be met for electronic or covert surveillance:

- Strong suspicion that a specific crime has been committed,
- Seriousness of the offence justifies surveillance,
- Investigative activities thus far have been unsuccessful and further enquiries would have no prospect for success.

The Law further stipulates **who** may be monitored, the **type** of surveillance allowed, the types of **authorisations** required, and the subsequent procedural **conclusions** and steps that must be taken for every piece of surveillance intelligence gathered.

2. Control Mechanisms

Effective control must include mechanisms that ensure that electronic surveillance is used in compliance with the law and that possible misuse is prevented. Some of these mechanisms are internal to the agency that requests the use of intrusive powers and several others external to the agency. Usually, the control procedures follow the process of requesting and approving a **warrant**. Depending on national legislation, warrants may be authorised by one or **several layers of control**:

- Internal Control
- Executive Control: Minister and/or Prosecutor
- Judicial Authorization
- Independent Authorization

Internal Control

Every request for a warrant must be first approved internally, within the police or intelligence service which wants to utilize special intrusive powers. Internal control usually involves several layers of authorization, starting with the direct supervisor who checks the necessity and appropriateness of the measure, a legal department that checks its legality, and ends with an approval given by senior management and engaging the responsibility of the institution for the warrant request.

Internal control provides an important deterrent to misconduct, showing that choosing to limit individuals 'rights to privacy is a serious decision that shouldn't be taken lightly.

Executive Control: Minister and/or Prosecutor

The first external control mechanisms is often a minister, responsible for the security service that requests the use of intrusive measures. In a few countries the minister is the highest and last authority who approves the use of intrusive methods. More often, a minister is the sole decision-maker on such issues only in emergency situations, clearly defined by law and limited in time.

Box 4. Executive Authorisation in France and the United Kingdom

In France, the interception of communication (metadata, geolocation, and content) is authorised by the Prime Minister. Also, all six intelligence agencies were created by executive decree.

Legislative framework in UK was revised in order to provide one single act on surveillance. In November 2016 the Investigatory Powers Act was adopted. It introduces new powers for UK intelligence agencies and law enforcement in targeted interception of communications, bulk collection of communications data, and bulk interception of communications. It requires communication service providers to retain UK internet users' "Internet connection records" (websites visited) for one year "communications service providers". It allows police, intelligence officers and a significant number of other government departments to see the Internet connection records, as part of a targeted and filtered investigation, without a warrant.

On the other hand, the Act creates an Investigatory Powers Commission, composed of a number of serving or former senior judges, with a mandate to oversee the use of all investigatory powers, alongside the oversight provided by the Intelligence and Security

To confine the possibilities for misusing intrusive powers at executive level (through collection of confidential information about political opponents, for example) laws

- must establish limits on what a minister can ask intelligence services to do;
- provide mechanisms for intelligence officers to report misconduct;
- require judicial authorisation as well as independent oversight to review the use of intrusive measures.

In some countries approval for the use of intrusive methods is entrusted to the public prosecutor. However, this is not a strong enough safeguard for individual rights, as the prosecuting authority might not be sufficiently independent of the investigation process to make an objective decision between the needs of the state and the right to privacy.

It should be noted that the roles of prosecutor and law enforcement offices differ substantially in Common Law systems (such as US, UK, India, Canada or Ireland) and in Civil Law systems (as in most European countries). In Common Law, police have relative autonomy over the investigative process and the prosecutor does not have the authority to issue warrants. In Civil Law, the public prosecutor plays a leading role in overseeing criminal investigations and often he is also able to authorise a warrant to conduct electronic surveillance.

Judicial Authorisation

Judicial authorization is considered to be one of the strongest safeguards for human rights. As noted in the Venice Commission report on democratic oversight of security services, judicial authorisation requirements subordinate security concerns to the law, and thereby institutionalize the respect for the law.

In consequence, a majority of European countries require security services to obtain **judicial warrants** before using methods of collecting information that are deemed to be particularly intrusive with regards to the right to privacy. Not all surveillance requires a warrant; when conducted in public or a community area (visual surveillance, body-worn video devices, police monitored CCTV), surveillance is typically regulated by law enforcement codes of practice and guidelines. However, when the subject of surveillance would hold a reasonable expectation of privacy (as in the case of focused electronic surveillance), a judicial warrant is required in most European countries.

Judicial warrants should be the product of an impartial evaluation. However, the secret nature of surveillance operations combined with rapid changes in technology and in the threat environment are challenging judicial supervision, often preventing judges from access to comprehensive information about the case.

Judicial warrants may be issued either to an intelligence agency for gathering information related with threats to national security, or to law enforcement agencies for collecting evidence in criminal investigations. In the latter case, the attainment of a warrant is essential for the admissibility of evidence in court.

Box 5. Warrant requirement in Canada

The Canadian Security Intelligence Service Act requires that intelligence service applications for judicial communication-interception warrants include the following information:

- the facts relied on to justify the belief that a threat to national security exists
- evidence that less intrusive techniques have been tried and have failed or reasons why they are unlikely to succeed
- the type of communication to be intercepted
- the type of information to be obtained
- the identity of the persons or classes of persons who are the targets of the investigation
- the identity of the persons, if known, whose communications will be intercepted
- a general description of the place, if known, where the warrant will be executed
- the period for which the warrant is being requested
- the details of any previous application made in relation to a person identified in the current application—including the date of the previous

Warrant requests made by law enforcement are usually authorised by a larger number of judges. However, intelligence services' requests for warrants are authorised by a few specialist judges (Canada, France, South Africa, Spain, among others) or by a higher court who deals with national security issues. Some countries have even created specialized courts to provide judicial authorisation for warrants on national security matters.

United States, for example, established the Foreign Intelligence Surveillance Court (FISC) to review government applications to conduct surveillance related to foreign intelligence investigations. FISC is comprised of eleven federal district court judges serving non-renewable terms of no more than seven years. They may approve electronic surveillance, certain physical searches, the use of a pen register or a trap and trace device, or access to certain business records. A second specialized court, the Foreign Intelligence Surveillance Court of Review hears government appeals against FISC decisions.

Sometimes, these specialised courts have the authority to review ongoing operations involving information collection, so they can limit collateral intrusion on unintended targets and ensure that covert, intrusive methods are not employed longer than necessary. In South Africa, judges may request interim written reports on the progress being made towards achievement of the objectives stated in the warrant.

Through these means of ex-ante and ex-post control of the use of intrusive methods of investigation, judges act as arbiters of government secrecy and individual freedoms in a very powerful way. Democratic systems assigns judges with this challenging task because they are regarded as independent, impartial and unlikely to be swayed by political considerations surrounding security services activities - as members of the executive power might be. Judges are also considered to be better suited to assess legal criteria such as necessity and proportionality, which are paramount when the measures sought may have significant human rights implications.

Independent Authorisation

Some countries have set up special independent commissions to authorise the use of electronic surveillance. The G10 Commission in Germany is named after the Article 10 of the Basic Law, stipulating the privacy of correspondence, post and telecommunication. The G10 Commission discusses the legitimacy of intervention in the rights provided by Article 10 by monitoring and reviewing the ministerial instructions to perform surveillance measures. This includes the collection, processing, and utilisation of personal data gathered by the intelligence services using covert methods. In addition, the G10 also decided on whether to inform those affected, after the surveillance ends without resulting in an indictment.

3. Oversight Mechanisms

The main purpose of oversight is to ensure that the implementation of laws, including the use of intrusive powers by security services, are in line with generally accepted democratic principles and individual rights and liberties. Effective oversight must observe four principles.

Independence. The first principle of oversight is that is has to be carried out by an authority independent from the one which carries out the intrusive measure. Therefore, oversight is exercised by a parliamentary committee and/or other expert oversight bodies (such as civil oversight bodies in Norway, Canada and Croatia).

Authority. Oversight can be hampered by the exemption of certain security services from the remit of oversight institutions, or the outsourcing to private actors of tasks traditionally performed by state security services. In addition, increased international cooperation in the field of counterterrorism and fighting organised crime can complicate the oversight of certain information sharing or joint operations.

Ability. Oversight of electronic surveillance requires a good understanding of the role of each security service , and especially the intelligence, in the national intelligence system. Oversight bodies must have access to sufficient funds and an experienced staff to conduct research and investigations.

Secrecy versus transparency. Oversight bodies must ensure a certain degree of transparency towards the public, while maintaining a necessary level of secrecy. Handling sensitive material in a confidential manner is essential for protecting the integrity of operational matters and for reassuring security services that oversight bodies are responsible, reliable partners.

The main bodies with an oversight mandate over the conduct of security services and their use of intrusive methods are:

- ✓ Parliamentary committees (for defence and security, intelligence control, human rights);
- ✓ Ombuds-institutions that receive and investigate citizens 'complaints on human rights infringements by security services;
- ✓ Data protection commissioners are independent national authorities responsible for upholding the right of individuals to data privacy through the enforcement and monitoring of compliance with data protection legislation.

Civil society organisations and media play an informal role in oversight, monitoring security services activities and the respect of human rights. They inform and often shape public debate, raising attention on abuses and maladministration, and exerting pressure on parliament and government bodies to define and implement relevant remedies.

What is the role of Parliament in the oversight of electronic surveillance?

Parliamentary oversight and judicial supervision have different strengths and weaknesses, which make them distinctive and complementary elements for an effective oversight of security services' use of intrusive methods for information collection.

- ✓ Parliamentary oversight is more policy-related, whereas judicial oversight deals exclusively with legal questions;
- ✓ Parliamentary oversight is, in theory, unlimited. Members of Parliament have the democratic legitimacy to request information and explanations about any aspect of the work of a governmental agency and have the right to inspect premises and check intrusive capacities themselves;
- ✓ Judges tend, sometimes, to be more differential to the executive branch in intelligence matters than Members of Parliament (at least those from opposition).
- ✓ Although parliaments tend to have very little authority over operational matters, they have broad powers to determine the mandate and budget of the security services, which gives them important leverage in influencing their conduct.

The oversight of intrusive methods for information collection is generally in the competency of standing committees for defence and security (as regards law enforcement agencies) and for intelligence oversight (as regards intelligence services).

Besides the classical legislative and oversight activities of parliamentary committees there are a few issues parliaments should consider when assessing the safeguards to the use of intrusive methods for information collection in their country.

Introducing Reporting Requirements in Legislation

Reports on the extent of the use and the implementation modalities of intrusive methods of investigation are extremely effective accountability mechanisms. They allow for ex-post judicial and parliamentary control, and, when not classified, ensure a necessary level of transparency towards the public. Several types of reports serve these purposes:

- ✓ Regular updates on the development and the results of surveillance are submitted to the judge who issued the warrant by the security personnel in charge of a case. The updates are often made orally

in front of the judge, or, a written report is handed personally to the judge, for strict protection of information confidentiality.

- ✓ Statistical reports are published, usually annually, by security services or/and by courts, providing information on the number of surveillance warrants implemented (for criminal investigations and national security), the number warrant requests rejected by relevant courts. Rarely, but significantly form an accountability perspective, such reports refer to the number of targets indicted, arrested, condemned – as result of surveillance warrants.
- ✓ Where legislation provides for this obligation of the security services (countries like Canada, Japan, Germany or Romania) reports include information about how many subjects of surveillance have been notified this has occurred, after the warrant expires and the surveillance does not lead to the indictment of the subject.

Regulating the Privatisation of Security

Increasingly, private security firms are conducting what are, or were once, essential law enforcement activities. It is important to consider and analyse the legal framework regulating the activities of private security companies, including private detectives or investigators. They should be subject to separate regulations, establishing a system of licensing which allows for certain limited and specified investigative activities.

Regulating and budgeting for changing technologies

Regulation of the use of surveillance changes regularly and is under frequent review. This is due to rapid development of technology and is also a response to domestic policy concerns. Inevitably, technological advancements are not always in the hands of the investigators before they are in the hands of criminals. Electronic evidence gathering is also a costly endeavour. Resource constraints limit the attainment and, thus, the use of hi-tech surveillance equipment and technologies by investigating authorities.

Responding to increased training needs for law enforcement officers and for judges

Knowledge of human rights legislation, security threats and risks, and technological advances in the implementation of surveillance and interception are imperative for all those involved in the use, approval and oversight of intrusive methods of investigation. Training in the laws, regulations and operative procedures for conducting covert electronic surveillance should be mandatory for *investigative officers* involved in managing such techniques. Moreover, *prosecutors and judges* are not always aware of the latest technological advances for the conduct of electronic surveillance. Training for judges should also cover issues of national security.

Box 6. Parliamentary Oversight in Belgium and Germany

Belgium's Intelligence Agencies Review Committee focuses on the legality and effectiveness of the intelligence services. It is empowered to "investigate the activities and methods of the intelligence services" including information collection. In 2010 the committee was tasked to supervise the use of newly acquired intrusive intelligence-collection capacities. The committee evaluates each intrusive surveillance operation and may order its termination (and the destruction of information collected) if it does not comply with the law. Furthermore, the committee is authorized to handle "complaints and denunciations…with regard to the operation, the intervention, the action or the failure to act of the intelligence services".

Germany's Parliamentary Control Panel, oversees the use of intrusive information-collection methods. The law requires the executive to provide them reports on the use of intrusive methods "at intervals of no more than 6 months". Based on these periodic reports, the panel prepares an annual report for the Bundestag on the nature and scope of the intrusive methods employed. Besides this monitoring function, the control panel has an authorization role: the Federal Intelligence Service must obtain their approval before intercepting international telecommunications traffic that is transmitted in "bundled

What resources are available on electronic surveillance safeguards?

Information about internationally accepted standards in in the use of electronic surveillance and the use of safeguards to protect rights of citizens is available in various formats.

Parliamentary Oversight of Security and Intelligence Agencies in the European Union was produced by the Directorate-General for Internal Policies of the European Parliament. This publication evaluated the oversight of national security and intelligence agencies

in order to identify good practices to be applied to European institutions.
http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf

Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime produced by the United Nations Office on Drugs and Crime is a practical, comparative study of electronic evidence gathering practices.
https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf

National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law was produced by the Directorate-General for Internal Policies of the European Parliament. The study found that large scale surveillance programmes operated by EU Members do not stand outside the realm of EU intervention but can be engaged from an EU law perspective.
http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf

The Right to Information and Privacy: Balancing Rights and Managing Conflicts was produced by the World Bank in conjunction with the Canadian International Development Agency. The paper ilustrates legislative and structural means to better define and balance the rights to privacy and the right to information.
http://wbi.worldbank.org/wbi/document/right-information-and-privacy-balancing-rights-and-managing-conflicts

The Democratic and Effective Oversight of National Security Services is published by the Council of Europe Commissioner for Human Rights and suggests means to make national oversight systems more effective in helping to promote human rights compliance and accountability in the work of security services.
https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2775460&SecMode=1&DocId=2286978&Usage=2

The National Security and European Case-Law Report was produced by the Research Division of the European Court of Human Rights. The report reviews the case law that has required national bodies to verify that proposed threat have had a reasonable basis. Member states are recognized to have a large measure of discretion when evaluating threats to national security.
http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Jurisprudence%20CEDH_En%20(final).pdf

The Right to Privacy in the Digital Age is a Report of the Office of the United Nations High Commissioner for Human Rights reviews the protection and promotion of human rights in the context of extended interception of digital communications and collection of personal data.
http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Overseeing Intelligence Services: A Toolkit is published by DCAF as a compendium of booklets providing detailed policy guidance on the oversight of intelligence services' work. It develops relevant topics such as Overseeing Information Collection (Tool 5), the Use of Personal Data (Tool 6) or Information Sharing (Tool 7). It is available in seven languages and includes guidance on the establishment and consolidation of intelligence oversight systems, reconciling secrecy and transparency, and handling complaints.
http://www.dcaf.ch/Publications/Overseeing-Intelligence-Services-A-Toolkit

Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU is published by the European Agency for Fundamental Rights. The report maps and analyses the legal frameworks on surveillance in the EU Members States, with a focus on mass surveillance. It also details oversight mechanisms introduced across the EU and presents the remedies available to individuals seeking to challenge such intelligence activities.
http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-summary-0_en.pdf

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) promotes good governance and reform of the security sector. The Centre conducts research on good practices, encourages the development of appropriate norms at the national and international levels, makes policy recommendations and provides in-country advice and assistance programmes. DCAF's partners include governments, parliaments, civil society, international organisations and the range of security sector services, including the military, police, judiciary, intelligence agencies, and border security services.
Visit us at www.dcaf.ch