Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 13293
03 September 2013

National security and access to information

Report[1]
Committee on Legal Affairs and Human Rights
Rapporteur: Mr Arcadio DÍAZ TEJERA, Spain, Socialist Group

Summary

The committee recalls the importance of the principle of transparency, including access to information held by public authorities, for democracy and good governance in general and for the fight against corruption in particular. It considers legitimate, well-defined national security interests as valid grounds for withholding information. At the same time, access to information forms a crucial component of national security, by enabling democratic participation, sound policy formulation and public scrutiny of State action.

The committee welcomes the adoption in June 2013, by a large assembly of experts from international organisations, civil society and academia and of national security practitioners, of the "Global Principles on National Security and the Right to Information" designed to give guidance to legislators and relevant officials throughout the world with a view to reaching an appropriate balance between public interests both in national security and in access to information. It supports the "Global Principles" and calls on the competent authorities of all member States of the Council of Europe to take them into account in modernising their legislation and practice concerning access to information.

The committee stresses a number of particularly important principles, including the need for robust oversight over the activities of secret services, the protection of bona fide disclosures of wrongdoings by "whistle-blowers" and the availability of a "public interest override" as a safeguard against overly broad exceptions from the general rule of free accessibility of all information held by public authorities. Information concerning the responsibility of State agents who have committed serious human rights violations such as murder, enforced disappearance, torture or abduction, does not deserve to be protected as secret.

1. Reference to committee: Doc. 12548, Reference 3762 of 15 April 2011.

Contents **Page**

A. Draft resolution 3
B. Draft recommendation 5
C. Explanatory memorandum by Mr Díaz Tejera, rapporteur 6
1. Introduction 6
1.1. Procedure 6
1.2. Overview of the main issues at stake 7
2. International human rights law governing access to information 7
2.1. Developments at national level 8
2.2. Developments at the European level 8
2.3. Case law of the European Court of Human Rights on access to information 11
3. Limitations on the right of access to information 12
3.1. The starting point: a presumption that all State-held information should be accessible 13
3.2. The public interest override 14
3.3. An independent body to decide on freedom of information requests 15
3.4. National security as an exception to access to information 15
3.5. Methods of classification of information 18
3.6. Logistical duties of public authorities in relation to access to information 19
3.7. Access to information and privacy 20
4. Oversight, review and complaints mechanisms 21
5. Protection of whistle-blowers 22
6. Conclusions 23

A. Draft resolution[2]

1. The Parliamentary Assembly recalls the importance of the principle of transparency, including access to information held by public authorities, for democracy and good governance in general and for the fight against corruption in particular.

2. It welcomes the fact that the Council of Europe was the first intergovernmental organisation to elaborate an international legal instrument on access to information, namely the Council of Europe Convention on Access to Official Documents (CETS No. 205), whilst recalling its Opinion 270 (2008) on the draft convention in which the Assembly had encouraged the Committee of Ministers to improve the text with a view to ensuring even greater transparency. The convention still requires four ratifications in order to enter into force.

3. The Assembly considers legitimate, well-defined national security interests as valid grounds for withholding information held by public authorities. At the same time, access to information forms a crucial component of national security, by enabling democratic participation, sound policy formulation and public scrutiny of State action.

4. Recalling its Resolution 1838 (2011) on abuse of State secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations and its Resolution 1675 (2009) on the state of human rights in Europe: the need to eradicate impunity, the Assembly stresses the need to place reasonable limits upon the invocation of national security as grounds to restrict access to information.

5. In particular, the Assembly reconfirms its position, expressed in paragraph 4 of Resolution 1838 (2011), that information concerning the responsibility of State agents who have committed serious human rights violations such as murder, enforced disappearance, torture or abduction does not deserve to be protected as secret. Such information should not be shielded from judicial or parliamentary scrutiny under the guise of "State secrecy".

6. The Assembly welcomes the adoption, on 12 June 2013, by a large assembly of experts from international organisations, civil society and academia and of national security practitioners, of the "Global Principles on National Security and the Right to Information" ("the Global Principles"), which are based on existing standards and good practices of States and international institutions. The Global Principles are designed to give guidance to legislators and relevant officials throughout the world with a view to reaching an appropriate balance between public interests both in national security and in access to information.

7. The Assembly supports the Global Principles and calls on the competent authorities of all member States of the Council of Europe to take them into account in modernising their legislation and practice concerning access to information.

8. The Assembly wishes to stress, in particular, the following principles:

8.1. As a general rule, all information held by public authorities should be freely accessible; in addition, business enterprises, including private military and security companies, have the responsibility to disclose information in respect of situations, activities or conduct that may reasonably be expected to have an impact on the enjoyment of human rights.

8.2. Exceptions from the rule of free access to information which are based on national security, or other equally important public interests such as the protection of international relations, health and safety or the environment, or on privacy interests, must be provided by law, pursue a legitimate purpose and be necessary in a democratic society.

8.3. Limitations to the rule of free access to information, including the rule of the neutrality of the Internet, should be interpreted restrictively. The burden of demonstrating the legitimacy of any restriction rests with the public authority seeking to withhold information.

8.4. Rules on the procedure for the classification and declassification of information and the designation of persons authorised to perform this task should be clear and publicly accessible. Information may be withheld on national security grounds for only as long as is necessary to protect a legitimate national security interest.

2. Draft resolution adopted unanimously by the committee on 24 June 2013.

8.5. As a safeguard against overly broad exceptions, access to information should be granted even in cases normally covered by a legitimate exception, where public interest in the information in question outweighs the authorities' interest in keeping it secret. An overriding public interest can typically be found where the publication of the information in question would:

8.5.1. make an important contribution to an ongoing public debate;

8.5.2. promote public participation in political debate;

8.5.3. expose serious wrongdoings, including human rights violations, other criminal offences, abuse of public office and deliberate concealment of serious wrongdoing;

8.5.4. improve accountability for the running of public affairs in general and the use of public funds in particular;

8.5.5. benefit public health or safety.

8.6. Information about serious violations of human rights or humanitarian law should not be withheld on national security grounds in any circumstances.

8.7. A person who discloses wrongdoings in the public interest (whistle-blower) should be protected from any type of retaliation, provided he or she acted in good faith and followed applicable procedures.

8.8. Requests for access to information should be dealt with in a reasonable time. Decisions to refuse access should be duly motivated, open to appeal before an independent body and ultimately subject to judicial review. Upon receipt of a request for information, a public authority should in principle confirm or deny whether it holds the requested information.

8.9. Public oversight bodies in charge of overseeing the activities of the security services should be independent from the executive and have relevant expertise, robust powers of investigation and full access to protected information.

9. The Assembly calls on all the member States of the Council of Europe which have not yet done so to sign and ratify the Council of Europe Convention on Access to Official Documents and to implement and, in due course, further improve the convention in the spirit of the Global Principles.

B. Draft recommendation[3]

1. The Assembly refers to its Resolution ... (2013) on national security and access to information and invites the Committee of Ministers to:

1.1. examine ways and means to promote the entry into force and speedy implementation of the Council of Europe Convention on Access to Official Documents (CETS No. 205);

1.2. to review the Council of Europe's own policies regarding access to information and classification and declassification of documents in light of the Assembly's resolution;

1.3. encourage member States of the Council of Europe to take into account the "Global Principles on National Security and the Right to Information," adopted on 12 June 2013 by an assembly of experts from international organisations, civil society, academia and national security practitioners, in particular concerning the points highlighted in the above-mentioned resolution, in modernising their legislation and practice.

3. Draft recommendation adopted unanimously by the committee on 24 June 2013.

C. Explanatory memorandum by Mr Díaz Tejera, rapporteur

1. Introduction

1.1. Procedure

1. On 22 March 2011, the Parliamentary Assembly decided to refer the motion for a resolution "National security and access to information" to the Committee on Legal Affairs and Human Rights, for report.[4] At its meeting on 6 June 2011, the committee appointed me as rapporteur.

2. At the hearing on media freedom in Europe, organised by the Sub-Committee on Media in Sweden on 12 September 2011, Dr Agnès Callamard, Executive Director of the non-governmental organisation (NGO) Article 19, addressed the parliamentarians on the issue of national security and access to information.

3. At its meeting on 6 September 2012, the committee considered an introductory memorandum[5] presenting the issues at stake and ongoing developments in this field.

4. Following an invitation by Open Society Justice Initiative (OSJI) and the Centre for Advanced Security Theory (CAST) at the University of Copenhagen, I attended an expert consultation on National Security and Right to Information in Copenhagen from 20 to 22 September 2012. This meeting discussed law and practices of European countries concerning the balancing of the public's right to know with the need for secrecy, on occasion, to protect legitimate national security interests and to contribute to the drafting of the "Global Principles on National Security and the Right to Information"[6] (hereinafter "the Global Principles") which were finalised on 12 June 2013. In Copenhagen, I presented the Council of Europe's *acquis* in this field, including the Assembly's earlier resolutions based on Mr Dick Marty's reports on rendition and secret detention.[7]

5. At its meeting on 11 December 2012, the committee held an exchange of views with three experts:

– Ms Sandra Coliver, Senior Legal Officer, Freedom of Information and Expression, at the Open Society Justice Initiative (OSJI), co-ordinating the project on "Global Principles on National Security and the Right to Information", New York, United States;

– Ms Susana Sanchez Ferro, Professor at the University of Madrid, Spain;

– Lord Alexander Carlile of Berriew CBE QC, former Independent Reviewer, London, United Kingdom.

Mr Matthew Pollard, Senior Legal Adviser, Amnesty International (London), also contributed to the discussion at the committee meeting.

---

4. Doc. 12548, Reference 3762 of 15 April 2011.
5. Document AS/Jur (2012) 27.
6. Global Principles on National Security and the Right to Information (also referred to as "Tshwane Principles" or "Global Principles"), issued 12 June 2013, drafted by 17 NGOs and five academic centres (Africa Freedom of Information Centre; African Policing Civilian Oversight Forum; Alianza Regional por la Libre Expresión e Información; Amnesty International; Article 19, the Global Campaign for Free Expression; Asian Forum for Human Rights and Development (Forum Asia); Center for National Security Studies; Central European University; Centre for Applied Legal Studies, Wits University; Centre for European Constitutionalisation and Security (CECS), University of Copenhagen; Centre for Human Rights, University of Pretoria (Tshwane); Centre for Law and Democracy; Centre for Peace and Development Initiatives; Centre for Studies on Freedom of Expression and Access to Information, Palermo University School of Law; Commonwealth Human Rights Initiative; Egyptian Initiative for Personal Rights; Institute for Defence, Security and Peace Studies; Institute for Security Studies; International Commission of Jurists; National Security Archive; Open Democracy Advice Centre; and Open Society Justice Initiative); facilitated by the Justice Initiative in consultation with the three special rapporteurs on freedom of expression of the United Nations, the Organization of American States (OAS) and the African Commission on Human and Peoples' Rights, the Representative on Freedom of the Media of the Organization for Security and Co-operation in Europe (OSCE) and the United Nations Special Rapporteur on Counter-Terrorism and Human Rights; available at: www.right2info.org/national-security/Tshwane_Principles.
7. Doc. 10957 , report on "Alleged secret detentions and unlawful inter-State transfers of detainees involving Council of Europe member States", 12 June 2006, Doc. 11302 , report on "Secret detentions and illegal transfers of detainees involving Council of Europe member States: second report", 11 June 2007; and Doc. 12714, report on "Abuse of State secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations", 16 September 2011.

1.2. Overview of the main issues at stake

6. Especially since the "war on terrorism" was launched in 2001, national security has frequently been invoked to limit freedoms and to cover up misconduct of public officials. Minimal access to secret information by parliament, the judiciary, but also the public, creates an imbalance of power in favour of the executive. This problem is rooted in the broader issue of lack of access to information held by the State, which is heightened by a "systematic and arbitrary invocation of the State secrecy privilege".[8]

7. Access to information is of fundamental importance in a democratic society. It is instrumental for the enjoyment of other human rights; it safeguards against abuses of power by enhancing transparency and accountability of government and it enables effective public participation of an informed society.[9]

8. The protection of the security of a nation and of its citizens is, of course, also an important public good. In order to protect the nation and conduct military and intelligence operations effectively, it is often necessary to keep some information from the general public. The inherent tension between withholding and allowing access to information is heightened by the lack of a clear legal framework and international standards, or of their effective implementation. Overly broad and vague national security exceptions from access to information allow for the cover-up of illegitimate activities and curtail victims' access to justice.[10]

9. Parliamentary and judicial oversight mechanisms are often not well equipped to properly balance these conflicting interests. This is either because they themselves do not have access to secret or classified information or, as far as parliamentary bodies are concerned, because parliamentary majorities supporting the government in place are usually reflected in the oversight bodies. Most human rights abuses in the context of the "war on terror" were in fact brought to light through whistle-blowers and investigative work by journalists and NGOs rather than through parliamentary or judicial oversight mechanisms.[11]

10. Whistle-blowers have thus gained importance in uncovering information of interest to the public, especially on human rights abuses committed under the guise of national security and State secrets. Unfortunately, some such whistle-blowers are now in custody facing charges of espionage.[12] For more details on this important subject, reference should be made to the valuable work of our Assembly colleague, Mr Pieter Omtzigt.[13] The above-mentioned "Global Principles" also include some important guidelines on the protection of whistle-blowers.[14]

11. Lack of information on important issues of public interest prevents effective scrutiny and fosters a culture of secrecy and impunity which, in turn, threatens the democratic values upon which our societies rest. We should therefore strive to create an enabling environment for the executive branch to respect, protect and ensure openness, thus avoiding the creation of a breeding ground for human rights abuses under the cloak of national security.

2. International human rights law governing access to information

12. An individual human right of access to information has been recognised at international level in various resolutions,[15] although it is typically regarded as an aspect of the right to freedom of expression.[16] The respective provisions on freedom of expression under the Universal Declaration of Human Rights (hereinafter "UDHR") and the International Covenant on Civil and Political Rights (hereinafter "ICCPR") both guarantee an individual right to seek and receive information, which makes up the right of access to information.[17] General Comment No. 34 affirms that Article 19 of the ICCPR "embraces a right of access to information held by public

8. Doc. 12714, op. cit., paragraph 45.
9. R. Peled and Z. Rabin, "The Constitutional Right to Information", 42 *Columbia Human Rights Law Review* 357, 2011, p. 357.
10. Global Principles (supra note 6), Introduction (Background and Rationale).
11. Doc. 12714, op. cit., paragraphs 2 and 50.
12. Ibid., paragraph 50; see the case of Bradley Manning, paragraphs 62-63 and 91 below.
13. See Resolution 1729 (2010), Recommendation 1916 (2010), and Report Doc. 12006 on the "Protection of 'whistle-blowers'", 14 September 2009, rapporteur: Mr Pieter Omtzigt.
14. See paragraphs 88-94 below.
15. See for instance United Nations General Assembly Resolution A/RES/59(I), 1946; OAS General Assembly Resolutions on Access to Public Information: Strengthening Democracy: AG/RES. 1932 (XXXIII-O/03), 10 June 2003; AG/RES. 2057 (XXXIV-O/04), 8 June 2004; AG/RES. 2121 (XXXV-O/05), 26 May 2005; AG/RES. 2252 (XXXVI-O/06), 6 June 2006; AG/RES. 2288 (XXXVII-O/07), 5 June 2007; AG/RES. 2418 (XXXVIII-O/08), 3 June 2008; AG/RES. 2514 (XXXIX-O/09), 4 June 2009; Declaration of Nueva Leon, 13 January 2004.
16. T. Mendel, "The Right to Information in Latin America: A Comparative Legal Survey", 2009, p. 1.
17. Article 19 of the UDHR; Article 19.2 of the ICCPR.

bodies".[18] The European Convention on Human Rights (ETS No. 5, "the Convention") provides for the right to receive information under the guarantee of freedom of expression,[19] although it is difficult to derive from the Convention a general right of access to information held by the State. The Organisation of American States and the African Union have recently adopted model laws on access to information to assist in the adoption of national legislation.

2.1. Developments at national level

13. The past few decades have seen the rapid development of freedom of information laws at national and regional level, providing for a subjective right of access to State-held information and official documents.[20] According to Open Society Justice Initiative, as of early June 2013, a total of 94 countries in the world have enacted some form of access to information provision or law[21] and another 20 States are in the process of drafting such laws.[22] Since the early 1990s, new or revised national constitutions have also included a right to information.[23] At the time of the drafting of this report, more than 5.2 billion people in 95 countries around the world enjoyed the right of access to information at least in law.[24] Of the 47 Council of Europe member States, only six, namely Andorra, Cyprus, Luxembourg, Monaco, San Marino and Spain, do not yet have laws on access to information.[25]

14. However, the quality of the national laws and their implementation vary widely,[26] which calls for the clarification of international standards, in particular as regards the exceptions from the rule of access to information in the name of national security.

2.2. Developments at the European level

2.2.1. The Council of Europe Convention on Access to Official Documents

15. The Council of Europe has affirmed the right of access to information on various occasions[27] and adopted the first international treaty on the right of access to public documents, the Council of Europe Convention on Access to Official Documents (CETS No. 205) in 2008.[28]

16. The most important achievement of the Convention is the recognition of the principle that access to official documents is the rule, and its refusal the exception.[29] The Convention gives "everyone" the right of access to official documents, irrespective of their motives or intentions. It also includes the first widely agreed definition of the notion of "official documents", which means "all information recorded in any form, drawn up or received and held by public authorities"[30] – thus including also information that was not produced by the public authority holding it, and whatever its form or format (written texts, audio or video recording, photographs, emails, information stored in electronic databases).[31]

---

18. General Comment No. 34 (July 2011), paragraph 18: www.right2info.org/resources/publications/general-comment-no.34/view.
19. Article 10 of the Convention.
20. J. Ackerman and I. Sandoval, "The Global Explosion of Freedom of Information Laws", 58 Admin. L. Rev. 85 2006, p. 85 ff.
21. Open Society Justice Initiative, www.right2info.org/resources/publications/laws-1/countries-with-foi-laws_march-2013.
22. http://right2info.org/laws.
23. Peled and Rabin, op. cit., p. 372 ff.
24. See Right 2 Info, "Constitutional Provisions, Laws and Regulations", 24 October 2011: www.right2info.org/laws/constitutional-provisions-laws-and-regulations.
25. Ibid.
26. An excellent overview on the basis of extensive empirical research is given in a report by Amanda Jacobsen (University of Copenhagen): www.right2info.org/resources/publications/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe.
27. See Committee of Ministers Recommendation No. R (81) 19 on "Access to information held by public authorities" of 25 November 1981; and Committee of Ministers Declaration on Freedom of Expression and Information, adopted on 29 April 1982.
28. Adopted by the Committee of Ministers on 27 November 2008 at the 1042bis meeting of the Ministers' Deputies, https://wcd.coe.int/ViewDoc.jsp?id=1377737&Site=CM.
29. Preamble of the convention, point 7 and Articles 2 and 3.
30. Article 1.2.*b* of the Convention.
31. See Explanatory Report, paragraph 11.

17. A weakness, from the point of view of this report, is the long list of possible limitations to the right of access in Article 3, including the protection of national security, defence and international relations, public safety, inspection, control and supervision by public authorities, even commercial and other economic interests, and the protection of the environment. I find it difficult to imagine how the protection of the environment could benefit from keeping information out of the public domain – the opposite would normally be the case. These exceptions are not defined in the Convention. But the sentence introducing the list of Article 3 requires that limitations "shall be set down precisely in law, be necessary in a democratic society and be proportionate to the aim".

18. This Convention has been criticised by several civil society organisations,[32] by some European States and by the Parliamentary Assembly of the Council of Europe for its narrow scope. Assembly Opinion 270 (2008) addressed to the Committee of Ministers,[33] drafted by Mr Klaas de Vries on behalf of our committee, took the unusual step of recommending that the Committee of Ministers ask the Steering Committee on Human Rights (CDDH) to reopen negotiations in order to:

– broaden the definition of "public authorities" to include a wider range of activities of public authorities and hence widen the scope of information made available;

– include a time limit on the handling of requests;

– clarify and strengthen the review process in case of the rejection of an information request.

19. The Committee of Ministers did not follow the Assembly's recommendation and the text was opened for signature as submitted to the Assembly. Nevertheless, the convention's very existence, even as a mere expression of the lowest common denominator, constitutes real progress for the right of access to information in international law. The declared objective of the convention is to lay down common minimum standards, which should be acceptable for as many States as possible, whilst all are encouraged to progress further towards the level of openness achieved by the most advanced States. It is noteworthy in this context that several so-called "new democracies", which had lived through decades of closed, oppressive regimes, are now in the vanguard of countries which have the most liberal laws on access to official documents, whilst some "established democracies" are lagging behind.[34]

20. In order for the Convention to enter into effect, ten ratifications are required. So far, six countries (Bosnia and Herzegovina, Hungary, Lithuania, Montenegro, Norway and Sweden) have ratified and another eight (Belgium, Estonia, Finland, Georgia, Monaco, Slovakia and Slovenia) have signed the convention but not yet ratified it. Four years after the opening for signature, this is a disappointing turnout, given that the text voluntarily refrained from being overly ambitious.

21. In my view, the Assembly should call on all member States which have not yet done so to sign and ratify the Convention on Access to Official Documents, in order to demonstrate their commitment in principle to transparency and good governance. Once the instrument enters into force, its follow-up body – the Group of Specialists on Access to Official Documents[35] will start to function and will be able to address outstanding issues on a case-by-case basis. This important work will be launched by the specialists appointed on proposal of those countries which have shown the keenest interest in transparency, by their early ratification of the instrument. The Group of Specialists can therefore be expected to set a progressive course, including on issues on which the Assembly, in its above-mentioned opinion, found the text of the convention too restrictive. The convention also foresees a mechanism for making proposals for amendments to the convention,[36] which will allow for improvements in light of the practical experience of the Group of Specialists.

22. On balance, therefore, I believe that the most realistic way for the Assembly to contribute to any real progress on this subject is to vigorously promote the ratification of the Council of Europe convention, so that it can begin to function. As national parliamentarians, we can put pressure on our governments as regards the

---

32. Mendel, op. cit., p. 13.
33. See also Doc. 11698, report on the "Draft Council of Europe Convention on Access to Official Documents", rapporteur: Mr Klaas De Vries.
34. According to a survey by Open Society Justice Initiative, requests for information from government bodies yielded more frequent and better quality responses in Armenia, Bulgaria and Romania than in France and Spain; Transparency and Silence, A Survey of Access to Information Laws and Practices in 14 Countries, Open Society Justice Initiative, New York/Budapest, 2006, p. 12
35. Article 11 of the convention.
36. Article 12 in conjunction with Article 19 of the convention.

signature and ratification of this instrument and hold them to account for the way they fill it with life. In my view, we should do this, rather than calling on the Committee of Ministers to start negotiating improvements to the convention before it has even entered into force.

2.2.2. Developments in the European Union

23. At the level of the European Union, Article 42 of the Charter of Fundamental Rights guarantees citizens "a right of access to documents of the Union institutions, bodies, offices and agencies, whatever their medium".[37] A similar right had already been recognised in Article 255 of the Treaty establishing the European Union (TEU), which was implemented by Regulation (EC) No. 1049/2001.[38] Since 2008, the European Commission and a group of member States have been trying to reduce the scope of the Regulation,[39] whilst the European Parliament[40] and another group of member States, supported by relevant NGOs, are resisting the proposed restrictions and are even lobbying in favour of further extending access to information to documents held by the European Union.[41] The Danish European Union Presidency attempted to broker a compromise solution on a limited package of reforms.[42] The Cypriot European Union Presidency pledged in July 2012 to take on the challenge of brokering a compromise solution on a limited package of reforms,[43] but a solution has still not been found at the end of the Irish Presidency in June 2013.

24. Access Info Europe made an interesting request in December 2008 for a document relating to the (still) ongoing reform of the European Union's transparency rules. The Council of the European Union provided Access Info Europe with the document containing member State proposals for reform, but with the names of the countries deleted, so it was impossible to know which country was putting forward which proposal. Access Info Europe challenged the Council's decision and on 22 March 2011 the (European Union) General Court ruled in favour of transparency. The Council, joined by the Czech Republic, France, Greece, Spain and the United Kingdom appealed this decision, whilst the European Parliament joined Access Info Europe in calling for a fully open legislative procedure. The Spanish Advocate General, Cruz Villalón, recently noted in his Opinion to the Court of Justice of the European Union, in Luxembourg, that the Council's legislative procedure should be as transparent as similar procedures at the national level, stating that "'legislating' is, by definition, a law-making activity that in a democratic society can only occur through the use of a procedure that is public in nature".[44] As a member of a legislative body, I must agree with him.

25. Another highly topical example for the need for greater transparency of the European institutions has arisen recently. Two requests by a Bloomberg News journalist for disclosure by the European Central Bank (ECB) of two internal papers[45] were refused by its President, Mr Mario Draghi. In short, these documents relate to allegations that, in the early 2000s, Greece arranged to disguise its debt levels through the use of cross-currency swaps with the United States investment bank Goldman Sachs. Purportedly this was to comply with criteria relating to public debt levels on which Greece's membership of the Eurozone depended.[46] When Bloomberg sued the ECB for access to these documents, the ECB successfully argued before the

37. http://eur-lex.europa.eu/en/treaties/dat/32007X1214/htm/C2007303EN.01000101.htm.
38. See Report of the Commission on the application in 2010 of Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0492:FIN:EN:PDF.
39. See Commission proposal for a regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents:
www.statewatch.org/news/2008/may/eu-access-reg-com-229-final.pdf
40. See European Parliament report on the proposal for a regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (recast):
www.statewatch.org/news/2011/nov/ep-access-to-eu-docs-revised-position.pdf.
41. See "EU Transparency – Campaign on the reform of EU access to documents regulation":
www.access-info.org/en/european-union/226-reforming-regulation-1049; see also the compilation of relevant materials by Statewatch: www.statewatch.org/foi/observatory-access-reg-2008-2009.htm.
42. See Access Info Europe, Last window of hope for EU transparency talks still open: Danish Presidency to broker agreement, 16 June 2012 (www.access-info.org).
43. See Access Info Europe, Cypriot Presidency prepares for agreement on access to EU documents, 9 July 2012.
44. See the full opinion: www.access-info.org/en/european-union/396-advocate-opinion.
45. The first paper was entitled "The impact on government deficit and debt from off-market swaps: the Greek case" and the second reviewed Titlos Plc, a structure that allowed the National Bank of Greece SA (ETE), the country's biggest lender, to borrow from the ECB by creating collateral.
46. "Greek Debt Crisis: How Goldman Sachs Helped Greece to Mask its True Debt", Beat Balzli, Spiegel Online, 8 February 2010.

(European Union) General Court that these documents should not be disclosed on the ground that "disclosure of those documents would have undermined the protection of the public interest so far as concerns the economic policy of the European Union and Greece".[47]

26. It would appear that the ECB feared that disclosure would undermine public confidence in Greece's ability to meet its debt obligations and thus threaten confidence in the single currency.[48] Personally, I believe that public confidence in the economic policies of the European Union, including the action taken by the ECB, would benefit rather than suffer from greater transparency. Vague assumptions about the impact on financial markets of the release of these documents are not, in my view, a legitimate bar to disclosure. I therefore sympathise with Bloomberg's disappointment with the ruling, which is clearly of concern to NGOs concerned with press freedom.[49] The European institutions' legally binding commitment to access to information in Article 42 of the Charter seems to be in danger of being overwhelmed by a new "culture of secrecy" in Brussels and in Frankfurt. An appeal brought by Bloomberg to the Court of Justice of the European Union is still pending.[50]

27. It should be noted that Mr Draghi, the current ECB president, was a Vice-Chairman of Goldman Sachs when the above-mentioned swaps were alleged to have been carried out. While Mr Draghi has denied any involvement,[51] the mere appearance of or potential for a conflict of interest should weigh heavily on the side of disclosure of documents potentially capable of settling the issue once and for all.

28. While the refusal to disclose these documents was not based on the national security exemption, it is recalled that all other public-interest grounds for restricting access should also meet the standards of the Global Principles.[52] The case demonstrates the need for reform of Regulation 1049/2001 in light of modern standards in order to prevent a culture of secrecy developing at the European level.

29. In my own view, it is very important that the European institutions set the best possible example for transparency and access to information. Public trust in politicians generally suffers from excessive secrecy. This is even more obvious in the case of European politics, which citizens unavoidably perceive as being more distant, more complex and more technocratic than their own local concerns.

2.3. Case law of the European Court of Human Rights on access to information

30. For many years, the European Court of Human Rights ("the Court") had not interpreted Article 10 of the European Convention on Human Rights (freedom of expression) as conferring an individual's general right of access to information held by the State.[53] More recently, the Court has cautiously modified its approach, on a case-by-case basis. In 2006, the Court examined a case where an environmental NGO had been refused access to documents regarding a nuclear power station. The Court held that the State's refusal to provide the information interfered with a right of the applicant to receive information derived from Article 10.[54] This approach was reconfirmed in two 2009 cases against Hungary. The Court found that the refusal of information requests – in the first case by the Hungarian Civil Liberties Union for documents relating to proceedings

---

47. Case T-590/10, *Thesing and Bloomberg Finance v. ECB*, Judgment of the General Court of 29 November 2012; "ECB Wins Ruling to Deny Access to Secret Greek Swap Files", Stephanie Bodoni, Elisa Martinuzzi and Gabi Thesing, Bloomberg, 29 November 2012.
48. "ECB Tells Court Releasing Greek Swap Files Would Inflame Markets", Elisa Martinuzzi and Gabi Thesing, Bloomberg, 14 June 2012.
49. "MLDI applies for permission to intervene in case against European Central Bank", Media Legal Defence Initiative, 31 May 2013; Transparency of the European Central Bank on the Financial Crisis: Access Info Europe applies to join key case at European Court of Justice, Access Info, 6 May 2013.
50. Appeal brought on 18 January 2013 by Gabi Thesing, Bloomberg Finance LP, against the judgment of the General Court (Seventh Chamber) delivered on 29 November 2012 in Case T-590/10: *Gabi Thesing, Bloomberg Finance LP v. European Central Bank*, O.J. C 101/9, 6 April 2013.
51. "Draghi Says He Knew Nothing About Goldman-Greece Deal", Jana Randow and Jeff Black, Bloomberg, 14 June 2011.
52. Global Principles, Introduction, p. 1.
53. *Leander v. Sweden*, Application No. 9248/81, judgment of 26 March 1987, paragraph 74; *Gaskin v. United Kingdom*, Application No. 10454/83, judgment of 7 July 1989, paragraph 52; *Guerra v. Italy*, Application No. 14967/89, judgment of 19 February 1998, paragraph 53; *McGinley and Egan v. United Kingdom*, Applications Nos. 21825/93 and 23414/94, judgment of 9 June 1998; *Roche v. United Kingdom*, Application No. 32555/96, judgment of 19 October 2005, paragraph 172 (but the Court found that the refusal of the information violated a positive obligation based on Article 8).
54. *Sdruženi Jihočeské Matky v. Czech Republic*, Application No. 19101/03, admissibility decision of 10 July 2006 (in the case at issue, the Court found that the refusal was sufficiently justified and covered by the restrictions of Article 10.2, therefore ruling the application inadmissible.

before the Constitutional Court and in the second by a historian for historical records held by the Hungarian State Security Service – violated Article 10.[55] In the first case, the Court still referred to its earlier, more restricted case law summed up in its judgment in the *Leander* case, but then went on to hold:

> *"Nevertheless, the Court has recently advanced towards a broader interpretation of the notion of "freedom to receive information" (see Sdružení Jihočeské Matky c. la République tchèque (dec.), no. 19101/03, 10 July 2006) and thereby towards the recognition of a right of access to information."*[56]

31. The Court confirmed this advance in a 2012 Grand Chamber judgment against Sweden, where it found that a University administrator's refusal to give the applicants – independent researchers – access to medical research data collected by the University "impinged on the [requesters'] right … to receive information in the form of access to the public documents concerned".[57]

32. It should further be noted that the Court has been the judicial pioneer of the principle that once information has been made public, restrictions on its further publication can no longer be justified, even on grounds of national security: in 1991, the Court ruled that the permanent injunction on a biography of a former member of the United Kingdom's security services could not be maintained as it had already been published in the United States, reasoning that prior dissemination meant that further publication could no longer adduce an identifiable harm.[58] This principle has been consolidated in the Internet age where information becomes public rapidly and irreversibly. It is also reflected in the Global Principles.[59]

33. In its Grand Chamber judgment in the case of *El-Masri v. the former Yugoslav Republic of Macedonia,*[60] concerning a German victim of the CIA's renditions and secret detentions programme,[61] the Court made great strides towards a recognition of a "right to the truth" of victims of human rights violations.[62] Referring to the Assembly's report, the Court also strongly criticised the secrecy in which the authorities shrouded the violations committed against Mr El-Masri:

> *"The concept of 'State secrets' has often been invoked to obstruct the search for the truth (see paragraphs 46 and 103 above). State secret privilege was also asserted by the US government in the applicant's case before the US courts (see paragraph 63 above). The Marty inquiry found, moreover, that 'the same approach led the authorities of 'the former Yugoslav Republic of Macedonia' to hide the truth' (see paragraph 46 above)."*[63]

34. In my view, the Court deserves praise and encouragement for continuing along the path of a case-by-case development of a human right to information. Such a right is an important precondition for the effective enjoyment of many other rights which are expressly recognised in the Convention, such as the right to life and freedom from torture (Articles 2 and 3), liberty and security (Article 5), respect for private life (Article 8), free speech (Article 10), even to free elections (Article 3, First Protocol).

3. Limitations on the right of access to information

35. As an aspect of the right of freedom of expression, the right of access to information is not absolute under the European Convention on Human Rights and may be subject to the limitations set forth in Article 10.2. These limitations include the protection of legitimate national security concerns, as it is stressed in the title of this report. But any limitation must be provided by law, pursue a legitimate purpose and be necessary in a democratic society.[64] As exceptions from the rule, limitations should be interpreted restrictively.

---

55. *Társaság A Szabadságjogokért (Hungarian Civil Liberties Union) v. Hungary*, Application No. 37374/05, judgment of 14 April 2009 and *Kenedi v. Hungary*, Application No. 31475/05, judgment of 26 May 2009.
56. *Társaság A Szabadságjogokért (Hungarian Civil Liberties Union) v. Hungary*, ibid., paragraph 35.
57. *Gillberg v. Sweden*, Application No. 41723/06, judgment of 3 April 2012 (Grand Chamber).
58. *The Observer and Guardian v. the United Kingdom*, Application No. 13585/88; *Sunday Times v. the United Kingdom (No. 2)*, Application No. 13166/87 – judgments of 26 November 1991
59. Global Principles, Principle 49.*b*.
60. Application No. 39630/09, judgment of 13 December 2012.
61. See reports by Mr Dick Marty, op. cit., Doc. 10957, section 3.1, and Doc. 11302 rev., point VI.i.
62. The Court discusses this aspect under the procedural aspect of Article 3 rather than Article 10, see paragraph 192: "The inadequate investigation in the present case deprived the applicant of being informed of what had happened, including of getting an accurate account of the suffering he had allegedly endured and the role of those responsible for his alleged ordeal", and paragraph 264: "The Court considers that the issue raised under this Article overlaps with the merits of the applicant's complaints under Article 3 and has already been addressed in relation to those complaints (see paragraph 192 above)."
63. *El-Masri v. the former Yugoslav Republic of Macedonia*, paragraph 191.
64. Article 10.2 of the Convention.

36. Given that national security is one of the weightiest public grounds for restricting information, when public authorities assert other grounds for restricting access in the public interest – including international relations, public order, public health and safety, law enforcement and economic interests of the State –, they should meet the same standards for imposing restrictions on access to information as those applying to national security considerations.[65]

37. In order to minimise ambiguity and disparities in the application of exceptions to the rule of free access to information held by public bodies, I see it as a core aspect of my mandate as rapporteur to contribute to the formulation and dissemination of some guiding principles in this respect. The project to formulate the afore-mentioned Global Principles has proved most helpful. As the Assembly's rapporteur, I have taken an active part in the formulation of these Principles, during the European consultation conference in Copenhagen in September 2012. I am pleased to note that my main points, and those of other European stakeholders, have been taken into account also in the formulation of the final wording of the Global Principles prepared in Pretoria (Tshwane) in April 2013.[66]

3.1. The starting point: a presumption that all State-held information should be accessible

38. In view of the principles of democracy and rule of law, the presumption should be that all State-held information is public and accessible.[67]

39. The Global Principles recall that in addition to the State and other public authorities, business enterprises within the national security sector, including private military and security companies, have the responsibility to disclose information in respect of situations, activities or conduct that may reasonably be expected to have an impact on the enjoyment of human rights.[68]

40. Authorities wishing to restrict access must provide a justification in conformity with Article 10.2 of the European Convention on Human Rights. The Global Principles confirm that in all cases the "burden of proof" for demonstrating the legitimacy of any restriction on access to information shall rest with the public authority seeking to withhold information.[69]

41. In addition to this general presumption, certain categories of information carry an even stronger presumption in favour of disclosure. These categories of information, which can be withheld on national security grounds only in the most exceptional circumstances, include the following:[70]

– violations of international human rights and humanitarian law; as regards gross violations of human rights or serious violations of international humanitarian law and systematic or widespread violations of the rights to personal liberty and security, such information may not be withheld on national security grounds in any circumstances;

– safeguards for the right to liberty and security of person, prevention of torture and inhuman and degrading treatment (prohibited by Article 3 of the Convention) and the right to life (enshrined in Article 2), in particular laws and regulations addressing the grounds, procedures for detention and the treatment of detainees, including interrogation methods;

– structures and powers of government, including laws and regulations applicable to those authorities and their oversight bodies and internal accountability mechanisms;

– decisions to use military force or acquire weapons of mass destruction, including information on the general size and scope of the intervention and the explanation of the reasons;

– information on surveillance: the legal framework on procedures to be followed for authorisation, usage, sharing, storing and destroying intercepted material;

– budgetary and financial information, including budget information sufficient to enable the public to understand security sector finances and procurement rules;

---

65. Global Principles, Principle 2.*b*.
66. See paragraph 4 above. I had asked our committee secretariat to accept the invitation extended by OSJI to participate in the finalisation meeting bringing together the results of the continental consultations for the formulation of the "Global Principles", now also known as the "Tshwane Principles". These consultations took place in Pretoria (Tshwane), South Africa, from 4 to 6 April 2013.
67. ARTICLE 19, The Public's Right To Know: Principles on Freedom of Information Legislation, 1999 (hereinafter "FOI Principles"), Principle 1.
68. Global Principles, op. cit., Principle 1.*b*.
69. Ibid., Principle 4.
70. Ibid., Principle 10 (providing further detail and examples).

– accountability concerning constitutional and statutory violations and other abuses of power;

– public health, public safety and the environment, including (as spelt out in Global Principle 10.H):

> *"1. In the event of any imminent or actual threat to public health, public safety, or the environment, all information that could enable the public to understand or take measures to prevent or mitigate harm arising from that threat, whether the threat is due to natural causes or caused by human activities, including by actions of the state or by actions of private companies;*
>
> *2. Other information, updated regularly, on natural resource exploitation, pollution and emission inventories, environmental impacts of proposed or existing large public works or resource extractions, and risk assessment and management plans for especially hazardous facilities."*

42. Even information deemed to be legitimately secret should only be withheld as long as it is "necessary in a democratic society", as it is formulated in Article 10.2. As information may lose its value, but also its "dangerousness" in case of publication due to the passage of time, appropriate consideration shall be given to the time factor and unnecessary or/and excessively long periods of classification must be avoided.

43. The notion of "public" or "State-held" information should be broadly defined to include information held by all public bodies in all branches of government, including the executive, legislative or judiciary as well as oversight institutions, intelligence agencies, the armed forces, police and other security agencies and any other bodies performing public functions and using taxpayers' money. Even if the nature of a given agency's work is more likely to fall within the general zone of exceptions, it should not be completely excluded from the obligation to disclose information from the outset.[71]

44. Furthermore, "exceptions should apply only where there is a risk of substantial harm to the protected interest and where that harm is greater than the overall public interest in having access to the information".[72] This is rightly reflected in various sets of soft law principles on access to information, including the Global Principles.[73]

45. Finally, the principle of disclosure of information concerning human rights violations applies regardless of whether the violations were committed by the State that holds the information or another State.[74] This means that member States of the Council of Europe should disclose information they hold about human rights violations committed by other countries, for example in the fight against terrorism.

3.2. The public interest override

46. The so-called "public interest override"[75] affirms a right of access to information which is normally covered by a legitimate exception in cases in which the public interest in the information in question outweighs the authorities' interest in keeping it secret. This "override" is an important safeguard, because it is not feasible to formulate exceptions in a sufficiently narrow way whilst covering any and all legitimately secret information.[76] The definition of "public interest" should be kept sufficiently open in order to allow for flexible interpretation.[77] An overriding public interest can typically be found where the information in question would:

– make an important contribution to an ongoing public debate;

– promote public participation in political debate;

– expose serious wrongdoings, in particular human rights violations by public officials;

---

71. FOI Principles, Principle 4; Global Principles, Principles 5 and 9.
72. See 2004 Joint Declaration by United Nations Special Rapporteur on Freedom of Opinion and Expression, Ambeyi Ligabo, OSCE Representative on Freedom of the Media, Miklos Haraszti, and OAS Special Rapporteur on Freedom of Expression Eduardo Bertoni: www.cidh.org/Relatoria/showarticle.asp?artID=319&IID=1. Note that the African Commission on Human and Peoples' Rights did not appoint a rapporteur on freedom of expression until 2005. In 2008, her mandate was expanded to expressly include the right to information.
73. Global Principles, Principle 3.*b*.ii; ARTICLE 19, Johannesburg Principles on National Security, Freedom of Expression and Access to Information, 1995 (hereinafter "Johannesburg Principles"), Principles 15 and 16; FOI Principles, Principle 4.
74. Global Principles, Principle 10.A.5.
75. See on this topic "The public interest test in FOI legislation", by Prof. Maeve McDonagh, Faculty of Law, University College Cork, Ireland, 2012: www.right2info.org/resources/publications/eu-mcdonagh-maeve-the-public-interest-test-in-foi-legislation/view.
76. T. Mendel, "The Johannesburg Principles: Overview and Implementation", 2003, p. 16.
77. R. Baxter, "Public Access to Business Information Held by Government", 1997 Journal of Business Law, p. 4.

– improve accountability for the running of public affairs in general and the use of public funds in particular;

– benefit public health or safety.[78]

3.3. An independent body to decide on freedom of information requests

47. The (unavoidably, despite our efforts) somewhat indeterminate character of the notion of public interest gives public authorities deciding on disclosure a wide margin of appreciation, in practice. For this reason, as well as to avoid a general chilling effect on disclosure, persons within public authorities who are responsible for responding to requests for information "should not be sanctioned for releasing information that they reasonably and in good faith believed could be disclosed pursuant to law".[79]

48. Refusals of requests for access to information must be reasoned and provide for the requester's right to a low-cost, expeditious review by an authority, which is institutionally, financially and operationally independent of the executive and all security sector authorities.[80] The refusing body should, in the event of non-disclosure, confirm or deny whether it does hold the information requested and give written reasons for denying disclosure.[81] Sufficient information as to which official(s) authorised non-disclosure and on the means of appealing should be provided.[82]

49. The independent reviewing authority "should have the competence and resources necessary to ensure an effective review, including full access to all relevant information, even if classified".[83] Its decisions should in principle also be open to challenge before a judicial authority.[84]

3.4. National security as an exception to access to information

3.4.1. Balancing the interests at stake

50. The protection of national security is central to the survival of every State and to the safety of the population at large. It goes without saying that many aspects of the work of the bodies responsible for the security of the State must remain removed from the public domain in order for such work to be successful. Information concerning working methods (tactics), identities of collaborators and informers etc. must remain secret. It is difficult to argue that there is a legitimate public interest to override such concrete security considerations.

51. But in many countries, a "culture of secrecy" has developed over time, shrouding in secrecy every aspect of the structures and activities of security-related agencies. This has effectively turned certain special services into a "State within a State", which is removed from any form of accountability. Such secrecy has been abused to cover up serious human rights abuses, placing the rule of law in jeopardy.[85]

52. The introduction of the Global Principles provides a good summary of the interests at stake:

> *"A clear-eyed review of recent history suggests that legitimate national security interests are, in practice, best protected when the public is well informed about the State's activities, including those undertaken to protect national security."*[86]
>
> *"Striking the right balance is made all the more challenging by the fact that courts in many countries demonstrate the least independence and greatest deference to the claims of government when national security is invoked. This deference is reinforced by provisions in the security laws of many countries that trigger exceptions to the right to information as well as to ordinary rules of evidence and rights of the accused upon a minimal showing or even the mere assertion by the government of a national*

78. M. Carter and A. Bouris, "Freedom of Information: Balancing the Public Interest", 2006, p. 8.
79. Global Principles, Principle 44.
80. Ibid., Definitions, p. 5 and Principle 26.
81. Ibid., Principles 19 and 20.*a*.
82. Ibid., Principle 20.*b*.
83. Ibid., Principle 26.*b*.
84. Ibid., Principle 26.*c*; on judicial oversight of the security sector, see section 4 below, paragraphs 83 to 87.
85. See Doc. 10957 on "Alleged secret detentions and unlawful inter-State transfers of detainees involving Council of Europe member States", Doc. 11302 rev on "Secret detentions and illegal transfers of detainees involving Council of Europe member States: second report"; and Doc. 12712 on "Human rights and the fight against terrorism".
86. Global Principles, Background and Rationale, p. 2.

security risk. A government's over-invocation of national security concerns can seriously undermine the main institutional safeguards against government abuse: independence of the courts, the rule of law, legislative oversight, media freedom, and open government."[87]

53. As I see it, these "institutional safeguards" are indeed part of "national security", understood in terms of the security of our democratic States as such.

3.4.2. The notion of national security

54. In view of the above, a restriction based on a national security interest should only be found legitimate in limited circumstances. The 1995 Johannesburg Principles on National Security, Freedom of Expression and Access to Information[88] are very strict, considering that a threat to national security corresponds to a threat to the country's existence and it is "necessary to protect the country's political independence or territorial integrity from the use, or threatened use, of force".[89]

55. The Global Principles have refrained from attempting to provide a positive definition of "national security". Such a definition, if intended to be universal, would indeed be as difficult as trying to define the notion of "terrorism", which the United Nations has been grappling with for decades.

56. Instead, Principle 2 includes a procedural recommendation, namely that "national security" should be defined precisely in national law, in a manner consistent with the needs of a democratic society.[90] In the same procedural vein, Principle 3, borrowing from the language of the European Convention on Human Rights and the case law of the Strasbourg Court, specifies:

"No restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: (1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest, and (2) the law provides for adequate safeguards against abuse, including prompt full, accessible and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts."

57. These criteria are spelt out clearly and, for me, convincingly:

"a. Prescribed by law. The law must be accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to understand what information may be withheld, what should be disclosed, and what actions concerning the information are subject to sanction.[91]

b. Necessary in a democratic society.

i. Disclosure of the information must pose a real and identifiable risk of significant harm to a legitimate national security interest.

ii. The risk of harm from disclosure must outweigh the overall public interest in disclosure.

iii. The restriction must comply with the principle of proportionality and must be the least restrictive means available to protect against the harm.

iv. The restriction must not impair the very essence of the right to information.

c. Protection of a legitimate national security interest. The narrow categories of information that may be withheld on national security grounds should be set forth clearly in law."

---

87. *Ibid*., Introduction, p 1.
88. Supra note 73.
89. Ibid., Principle 2.*a*; S. Coliver, Commentary to: The Johannesburg Principles on National Security, Freedom of Expression and Access to Information, *Human Rights Quarterly* 20 (1998) 12-80, p. 20.
90. Ibid., Principle 2.*c*; Similarly, M. Martin Scheinin, United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, in his report: 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, A/HRC/14/46, 2010, at Practice 1, commented: "While the understanding of national security varies among States, it is good practice for national security and its constituent values to be clearly defined in legislation adopted by parliament"; The 2004 Joint Declaration of the United Nations Rapporteurs on Freedom of Expression and of the Media states that "secrecy laws should define national security precisely and indicate clearly the criteria which should be used in determining whether or not information can be declared secret, so as to prevent abuse of the label 'secret' for purposes of preventing disclosure of information which is in the public interest".
91. See also, supra note 47.

58. As regards substance, the Global Principles begin with a "negative" definition.

> *"A national security interest is not legitimate if its genuine purpose or primary impact is to protect an interest unrelated to national security, such as protection of government or officials from embarrassment or exposure of wrongdoing; concealment of information about human rights violations, any other violation of law, or the functioning of public institutions; strengthening or perpetuating a particular political interest, party or ideology; or suppression of lawful protests."*[92]

59. I am pleased to note that the Global Principles reflect the Parliamentary Assembly's position that information related to human rights violations is not a legitimate State secret,[93] which I defended at the Copenhagen consultation in September 2012.

60. The Global Principles give examples of when access to information may be curtailed, but to which the general public interest override and other protections of access may still apply:[94]

– ongoing defence plans, operations, and capabilities for the length of time that the information is of operational utility (the Principles state that this means a requirement for disclosure of information once the information no longer reveals anything that could be used by enemies to understand the State's readiness, capacity or plans);

– information about the production, capabilities or use of weapons systems and other military systems, including communications systems;

– information about specific measures to safeguard the territory of the State, critical infrastructure, or critical national institutions (*institutions essentielles*) against threats or use of force or sabotage, the effectiveness of which depend on secrecy;

– information concerning national security matters pertaining to, or derived from, the operations, sources and methods of intelligence services;

– information concerning national security matters that was supplied by a foreign State or inter-governmental body with an express expectation of confidentiality and other diplomatic communications insofar as they concern national security matters.

61. Personally, I had suggested some modifications at the drafting stage, proposing to include also information concerning the prevention of terrorist acts and similar crimes and information pertaining to the fight against terrorism within the category of information to which access can be curtailed. This has now been taken care of in an explanatory note to Principle 9, which points out that:

> *"To the extent that particular information concerning terrorism, and counter-terrorism measures, is covered by one of the above categories, the public's right of access to such information may be subject to restrictions on national security grounds in accordance with this and other provisions of the Principles."*

62. Regarding diplomatic communications, I had pleaded for limiting the secrecy protection to those diplomatic communications which directly concern national security matters. This is now reflected in Global Principle 9. Many "confidential" embassy reports are in fact little more than compilations of press clippings – I do not see how their publication could cause any harm. Even the publication, through "Wikileaks", of numerous US embassy cables does not seem to have caused any serious diplomatic repercussions or lasting damage – on the contrary: many of the cables that the US Government seems to be most embarrassed about actually show that US diplomats in the field are nobody's fool and report home in a refreshingly realistic and candid way. One lesson learnt from this massive leak is in fact that the publication even of relatively sensitive information is nowhere near as damaging as had previously been assumed. I therefore consider the extreme severity with which the US authorities are treating Mr Bradley Manning, the young soldier who seems to be the "source" of these leaks, as most inappropriate.[95]

63. A final ground for departing from the access to information may be a "state of emergency", which has been proclaimed in accordance with national and international law, and which threatens the existence of a State.[96] This ground should be used with the same circumspection as the recourse to the "state of emergency" in general. Any derogation from the right to information must be consistent with other obligations

92. Global Principles, Definitions, p. 6. This is also the approach followed by the Johannesburg Principles, Principle 2.
93. See Resolution 1838 (2011), paragraph 4.
94. Global Principles, Principle 9.
95. See for example www.reuters.com/article/2013/02/28/us-usa-wikileaks-manning-idUSBRE91R0T720130228.
96. Global Principles, Principle 8.

under international law. The notes to Principle 8 rightly point out that certain aspects of the right to seek, receive and impart information and ideas are closely related to the enjoyment of certain non-derogable rights (such as the right to life or the prohibition of torture) and must therefore be respected also in times of emergency.

3.5. Methods of classification of information

64. While information may be classified following narrow and legal criteria, States use different methods of classification, including the systematic or automatic classification of all documents following pre-established criteria and a case-by-case approach.[97] From a freedom of information perspective the legal criteria for classification should be sufficiently clear and narrowly framed and the method should provide for appropriate procedural safeguards. For example, the law should specify which individuals are authorised to classify information and that they should be traceable or identifiable from the classified document to facilitate accountability.[98]

65. When a document is classified, it should be marked as such; there should be a record providing a justification referring to the level and the duration of the classification and specifying the harm that could result from disclosure.[99] There should be a possibility for public personnel to internally challenge classification if they feel it is improper or no longer justified.[100] Further, classified status as such should not exempt information from being considered for disclosure following a request.[101]

66. There must be time limits placed on classification, which accord with the principle that information should only be withheld as long as it is "necessary in a democratic society", as it is formulated in Article 10.2 of the Convention. To guarantee the fulfilment of this principle, periodic review of the classification of information should take place at least every five years, with the absolute rule that no information should be classified indefinitely. At the point of classification, the relevant personnel should specify the date, conditions or event upon which classification lapses to make the review process efficient and effective.[102]

67. The Council of Europe's declassification policy, adopted by the Committee of Ministers in 2001,[103] sets a positive example in this respect: whilst a large number of documents are public from the start, those classified as "restricted" automatically become public after one year, and the small number of "confidential" or "secret" documents after ten and thirty years respectively, unless a specific decision is taken to make an exception from this rule. The Parliamentary Assembly, and in particular the Committee on Legal Affairs and Human Rights, has a fairly liberal policy too. Whilst most documents are initially classified as "restricted", draft reports enter the public domain as soon as they are adopted at committee level, and the committee freely "declassifies" other documents whenever the rapporteur so requests.

68. The general public should have access to the procedures and standards of the country's classification system,[104] as well as to an index of classified information.[105]

69. Under Article 7 of the European Convention on Human Rights (no punishment without law), it would appear to be obvious that any criminal sanctions for the violation of State secrets require that the lists of items protected as State secrets referred to in general provisions of criminal law penalising breaches of State secrecy must themselves be available to the public, and that the use of information which is already in the public domain cannot be penalised as a breach of State secrecy. The report by our former colleague Christos Pourgourides on "Fair trial issues in criminal cases concerning espionage or divulging State secrets"[106] shows that this does not go without saying everywhere: in the Russian Federation, several scientists were sentenced to long prison terms for having "disclosed" information that was undisputedly already in the public domain before the scientists in question used it in the framework of their academic research and publication activities.

---

97. T. Mendel, Defining the Scope of National Security: Issues Paper for the Open Society Justice Initiative National Security Principles Project, May 2011, p. 6f.
98. Global Principles, Principle 13.
99. Ibid., Principle 11.
100. Ibid., Principle 14.
101. Ibid., Principle 18.
102. Ibid., Principle 16; see also: Open Society Justice Initiative, Declassification Procedures in Council of Europe Member States (2012).
103. Resolution Res(2001)6.
104. Global Principles, Principle 12.
105. Ibid., Principle 15.
106. Doc. 11031, "Fair trial issues in criminal cases concerning espionage or divulging State secrets", 25 September 2006.

70. Similarly, the United States' Government relied on the State secrecy privilege in order to prevent civil claims brought by "renditions" victims such as Khalid el-Masri to be heard in court. Whilst the government argued that the trial would require discussing State secrets related to the fight against terrorism, the Assembly's rapporteur, Dick Marty, pointed out in an *amicus curiae* brief he submitted to the United States Supreme Court that all the information needed to sustain the Mr el-Masri's case was already in the public domain – specifically, in the Assembly's own reports on renditions and secret detentions,[107] which covered Mr el-Masri's case quite extensively.

71. The above cases in Russia and in the United States would have violated the Global Principles. As regards the cases of the Russian academics, the Principles hold that persons who do not have access to classified information shall not be subject to prosecution for the violation of State secrecy laws[108] and that any such laws or other legal regulations must be public.[109] These provisions are mainly intended to protect journalists, but they also cover, for example, academic or NGO researchers. At the same time, as the Principles make it clear, this is not intended to guarantee impunity to journalists and other researchers who commit other criminal offences in order to obtain the secret information which they do not have access to. We do not need to go to the extreme example of a journalist or researcher torturing or otherwise blackmailing a "source" into giving him or her access to secret information: a break-in committed in order to gain access to desired information remains punishable as such.

72. I agree with the drafters of the Principles that "[t]hird party disclosures operate as an important corrective for pervasive over-classification". My position is also in line with that of the Special Rapporteurs of the United Nations and the Inter-American Commission on Human Rights, who in their 2010 Joint Statement on Wikileaks stated that:

> *"[P]ublic authorities and their staff bear sole responsibility for protecting the confidentiality of legitimately classified information under their control. Other individuals, including journalists, media workers and civil society representatives, who receive and disseminate classified information because they believe it is in the public interest, should not be subject to liability unless they committed fraud or another crime to obtain the information."*[110]

73. In the same vein, it is only logical that persons without access to classified information cannot be compelled to reveal the sources of such information.[111]

3.6. Logistical duties of public authorities in relation to access to information

74. While one of the most significant threats to the right of access to public information is the veil of the illegitimate national security exemption, public authorities have important ancillary duties, which must be fulfilled in order to guarantee the practical effectiveness of the right to information.

75. When requests for information are made, public authorities must devote sufficient resources and time to locate missing information, no matter the reason for its disappearance.[112] Further, procedures carried out to locate the information should be subject to judicial review, along with the reasons for the disappearance. If information cannot be found, police or administrative authorities should investigate the disappearance and publish the outcome.

76. It is recommended that time limits for responding to requests for information are set down by law and are not more than 20 or at most 30 working days.[113] The law can foresee different time limits to account for differing complexity and volumes of information. Where information is required urgently to "safeguard the life and liberty of a person", expedited time limits should apply.

---

107. See note 7 above.
108. Global Principles, Principle 47.
109. Ibid., Principle 3.*a*.
110. Joint Statement On Wikileaks by UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank LaRue, and Inter-American Commission on Human Rights, Special Rapporteur for Freedom of Expression, Catalina Botero Marino, 21 December 2010.
111. Global Principles, Principle 48.
112. Ibid., Principle 21.
113. Ibid., Principle 25.

77. It is not a bar to access to information that part of a requested document is legitimately withheld or classified, if parts of it can be disclosed. On such occasions, "public authorities have an obligation to sever and disclose the non-exempt information".[114] Moreover, even legitimately withheld information should be identified with as much specificity as possible.[115] Where possible, disclosed information should be made available in the format requested.[116]

78. All of these duties apply to information supplied to oversight bodies, as well as to members of the public. If they are not fulfilled, the practical effect is the same as where an illegitimate national security exemption is applied. Unreasonable logistical excuses are therefore just as unacceptable as unfounded refusals to release information on grounds of national security.

3.7. Access to information and privacy

79. Liberal access to information held by public bodies of the kind advocated in this report may well clash with the right to privacy of those directly concerned by the information. The right to privacy is also protected by the European Convention on Human Rights (Article 8). At the same time, access to information often complements the right to privacy in making government more accountable, including for breaches of the same right.[117] An individual's right to access information held by public authorities on him- or herself in effect serves to protect his or her right to privacy: it enables the individual to control the use of personal data and to rectify any inaccurate information. Conflicts usually arise due to a lack of understanding of what information is actually intended to be accessed or needs to be protected, and whenever government officials invoke a claim to privacy in order to shield their own improper use of public authority or other wrongdoings.[118] While the issue is definitely of key importance in determining the scope of the right to information, I intend to deal with it only insofar as it is relevant to the relationship between access to information and national security. Different aspects of access to information and the right to privacy have been the subject of other work of the Parliamentary Assembly.[119]

80. International human rights law does not give priority to one of the two rights – access to information and protection of privacy – over the other. They must be balanced against one another on a case-by-case basis.[120] Firstly, clear and compatible definitions of protected personal information must be laid down in legislation and applied by relevant oversight mechanisms. Secondly, balancing tests weighing the competing interests should take into account both private and public interests. Finally, it must be borne in mind that a government as a collegiate body cannot invoke a right to privacy of its own accord. Only if personal information pertaining to the personal life of a public official is involved may the person concerned claim a right to privacy, which must then be weighed against the interests of those accessing and using that information. Where personal data relate to criminal wrongdoings or other human rights abuses, the public interest in transparency and accountability of public bodies may well override an official's right to privacy. This said, the presumption of innocence (Article 6.2 of the Convention) requires that information on allegations of criminal wrongdoings must be treated with utmost care in order to ensure that the suspect's right to a fair trial is not violated by the publication of incriminating information and its discussion outside the courtroom.

81. Also, victims of human rights violations may well have a legitimate privacy interest in avoiding the public disclosure of their names, in order to prevent further harm. This point is explained very pertinently in a note to Principle 10.A.6.*b*:

> *"The names and other personal data of victims, their relatives and witnesses may be withheld from disclosure to the general public to the extent necessary to prevent further harm to them, if the person concerned expressly and voluntarily requests withholding, or withholding is otherwise manifestly consistent with the person's own wishes or the particular needs of vulnerable groups. Concerning victims of sexual violence their express consent should be required. Child victims (under age 18) should not be identified to the general public. This principle should be interpreted, however, bearing in mind the reality that various governments have, at various times, shielded human rights violations from public view by invoking the right to privacy, including of the very individuals whose rights are being or have been grossly violated, without regard to the true wishes of the affected individuals."*

---

114. Ibid., Principle 22.
115. Ibid., Principle 23.
116. Ibid., Principle 24.
117. D. Banisar, "The Right to Information and Privacy: Balancing Rights and Managing Conflicts", 2011, pp. 3 and 9.
118. Ibid., p. 9.
119. See, for example, Doc. 12695 , report on "The protection of privacy and personal data on the Internet and online media", 29 July 2011; Report Doc. 8130 and Resolution 1165 (1998) on the right to privacy, 3 June 1998.
120. D. Banisar, op. cit., p. 16.

4. Oversight, review and complaints mechanisms

82. Procedures to review denials of requests for access to information and complaints mechanisms should ensure both that non-confidential information is accessible and that legitimately confidential information is protected.

83. Oversight bodies, both in the judicial and parliamentary spheres, and independent review and complaints bodies are crucial for maintaining a system of checks and balances in the security sector. Such bodies should be based in law and cover all aspects of the security sector. This includes compliance with the law, including human rights law, the effectiveness and efficiency of intelligence operations, and administrative and financial practices.[121] Further, where there is sufficient evidence to suggest that a criminal offence has been committed, an effective investigation and, as appropriate, criminal prosecution should be provided for. National security considerations must not lead to *de facto* impunity for State officials involved in security-related operations.

84. The difficulty, to date, has been the lack of information provided to these bodies[122] and the lack of expertise and understanding ascribed to them.[123] It is therefore essential that oversight institutions have full and unhindered access to all information necessary for the fulfilment of their mandate.[124] They must receive full co-operation from the respective security agencies, be able to conduct investigations and reviews at their own initiative and be vested with the necessary powers and human and financial resources to perform their duties effectively.[125]

85. Another difficulty lies in the fact that oversight institutions are national bodies whose competences are limited to overseeing the actions of their own countries' security sector. At the same time, international co-operation between security bodies is becoming increasingly prevalent, in response to the fact that security threats are also transcending national boundaries. Frequently, intelligence is shared on the express condition that the recipient service must not disclose the information provided or its source. The results of any such co-operation are therefore, in fact, not subject to oversight. A solution should be sought in improved international co-operation between national oversight bodies, to match the development of co-operation at the operational level.[126] In theory, this should not be a problem among institutions from countries subjected to the same standards for transparency and the protection of human rights. In practice, this still requires much progress in the organisational cultures prevailing in the security sectors in many, if not all, member States of the Council of Europe.

86. It is noteworthy that security sector oversight bodies are public in nature and that, consequently, they are in principle themselves included in the ambit of the right of access to information.[127]

87. In order to achieve the best possible results in balancing transparency and national security interests, it has been suggested, in a previous report of the Assembly, to structure oversight bodies in such a way that they are made up of professional judges, who are assisted by experts on the functioning of security services. This body should have unrestricted access to any and all information held by the executive in order to be able to decide which information should remain confidential and which should be published. The procedure before this body should itself be confidential, but adversarial, in order to allow balanced and fully informed decisions to be taken.[128]

---

121. M. Scheinin, op. cit., Practice 6.
122. For example, in *R. (Khan) v. Secretary of State for Foreign and Commonwealth Affairs* [2012] EWHC 3728 (Admin), a British administrative court was unable to examine, even under closed material procedure, the legality of British intelligence being passed to the United States to facilitate drone strikes in the Middle East, because the British Government followed its policy of neither confirming nor denying the existence of such intelligence or whether it was transferred to the United States. Therefore, the court was unable to examine the question before it (the court accepting that the government was entitled to refuse to furnish the court with this information).
123. Inter-Parliamentary Union (IPU) and the Centre for the Democratic Control of Armed Forces (DCAF), Parliamentary Oversight of the Security Sector, 2003, p. 20.
124. M. Scheinin, op. cit., Practice 7; Global Principles, Principle 32.
125. M. Scheinin, ibid.; Global Principles, Principle 33; Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, A New Review Mechanism for the RCMP's National Security Activities, 2006, p. 18.
126. See the third report by Mr Dick Marty (Doc. 12714), paragraphs 52-57.
127. Global Principles, Principle 34.
128. See Assembly Doc. 12714, op. cit.; see in this connection also the controversy in the United Kingdom on "closed material procedure", for example, Rosalind English, "Secret justice: do we have a compromise?", UK Human Rights Blog, 4 April 2012, and the exchange with David Anderson QC, independent reviewer of United Kingdom antiterrorism legislation. These matters recently came to a head when the Supreme Court of the United Kingdom "reluctantly" decided

5. Protection of whistle-blowers

88. In order for the public as a whole to benefit from whistle-blowing as a "tool to increase accountability and strengthen the fight against corruption and mismanagement," as the Assembly formulated it in its Recommendation 1916 (2010) on the protection of "whistle-blowers", public personnel should be protected from retaliation when they disclose information showing wrongdoing, regardless of its level of classification and the potential impact on national security.[129] Specifically, they should be protected from civil or criminal liability, the loss of their job and/or physical and emotional harm.[130] Furthermore, they should not be required to produce documentary evidence for their claims to be investigated or to avoid retaliation, nor should they bear the burden of proof in relation to the veracity of the disclosure, provided they acted in good faith.[131]

89. The Global Principles provide a comprehensive list of categories of information which whistle-blowers should be able to disclose without suffering retaliation, including information on:[132]

– criminal offences;

– human rights violations;

– international humanitarian law violations;

– corruption;

– dangers to public health and safety;

– dangers to the environment;

– abuse of public office;

– miscarriages of justice;

– mismanagement or waste of resources;

– retaliation for disclosure of any of the above-listed categories of wrongdoing;

– deliberate concealment of any matter falling into one of the above categories.

90. Even if the disclosed information does not fall within one of these categories, whistle-blowers should be able to rely, as the case may be, on the "public interest override" (see section 3.2, paragraph 46 above) or the "public interest defence"[133] as recognised by the Global Principles. Any measures against them should be limited to civil ones. Criminal prosecution of whistle-blowers should only take place in the most exceptional of circumstances, be prescribed by law and be proportionate to the harm caused to interests of national security.[134]

---

to hear part of an appeal without the presence of a party to a case on grounds of national security (www.supremecourt.gov.uk/news/bank-mellat-v-hm-treasury.html); Adam Wagner, "Historical first as Supreme Court boots Iranian bank out of secret hearing", UK Human Rights Blog, 21 March 2013.

129. Global Principles, Part IV.

130. Ibid., Principle 41.

131. Ibid., Principle 38.

132. Ibid., Principle 37.

133. Ibid., Principle 43: "Public Interest Defence for Public Personnel

a. Whenever public personnel may be subject to criminal or civil proceedings, or administrative sanctions, relating to their having made a disclosure of information not otherwise protected under these Principles, the law should provide a public interest defence if the public interest in disclosure of the information in question outweighs the public interest in non-disclosure

b. In deciding whether the public interest in disclosure outweighs the public interest in non-disclosure, prosecutorial and judicial authorities should consider:

a. i. whether the extent of the disclosure was reasonably necessary to disclose the information of public interest;

b. ii. the extent and risk of harm to the public interest caused by the disclosure;

c. iii. whether the person had reasonable grounds to believe that the disclosure would be in the public interest;

d. iv. whether the person attempted to make a protected disclosure through internal procedures and/or to an independent oversight body, and/or to the public, in compliance with the procedures outlined in Principles 38-40; and

e. v. the existence of exigent circumstances justifying the disclosure."

134. Ibid., Principle 45; see also the following two judgments of the European Court of Human Rights upholding the protection of whistle-blowers:

– *Bucur and Toma v. Romania* (2013), Application No. 40238/02

91. The current harsh criminal prosecution against the "Wikileaks" source, Bradley Manning, seems to be a clear violation of the above-mentioned principles. The publication of the video recording of the manhunt by a US helicopter crew in Baghdad targeting civilians, including journalists, whilst making cynical comments clearly concerns criminal offences, human rights violations and violations of international humanitarian law committed by the helicopter crew. Helping to make this public in order to generate a public debate and contribute to accountability for such actions should be commended, not punished. Any criminal sanctions for these alleged leaks should be proportionate with the actual harm done and should take into account the idealistic motivation of Mr Manning, who was barely over twenty years old at the time of the alleged deeds.

92. To maximise the benefits provided by whistle-blowers to the general public, whistle-blower protection laws should establish internal procedures and designate persons within public authorities who are mandated to receive protected disclosures.[135] In addition, if internal mechanisms either do not exist or are dysfunctional, whistle-blowers should be able to make protected disclosures to independent oversight bodies, which protect the identity of whistle-blowers to safeguard them against even the most subtle forms of retaliation.[136] Public disclosures, with all the potential risks attached to them, should take place only as a last resort.

93. To ensure the universal protection of public personnel, such employees should not be able to waive or contract out of whistle-blower protection. Any such agreement or contract should be considered void *ab initio*.[137] Whistle-blowers should be able to report retaliation or the threat thereof to independent oversight bodies which have the function of taking remedial or restorative measures.[138]

94. These requirements safeguard the protection of whistle-blowers and the wider aims of preventing abuses of power and facilitating accountability of governments, including the security sector. They should be enshrined in guidelines applicable to all public authorities for the purpose of increasing legal certainty and to reassure prospective whistle-blowers.[139]

6. Conclusions

95. The increased scope of special operations undertaken and relevant provisions enacted for reasons of national security, especially since 9/11, have had a negative impact on access to information laws aimed at improving transparency and accountability. The resulting lack of information has, in turn, prevented parliaments, courts and ordinary citizens from participating in a meaningful way in relevant decisions and from holding public authorities to account for their actions.

96. The Preamble of the Global Principles rightly stresses that:

> *"Access to information, by enabling public scrutiny of State action, not only safeguards against abuse by public officials but also permits the public to play a role in determining the policies of the State and thereby forms a crucial component of genuine national security, democratic participation, and sound policy formulation. In order to protect the full exercise of human rights, in certain circumstances it may be necessary to keep information secret to protect legitimate national security interests."*

97. Adequate safeguards must therefore be put in place at different levels of procedure in order to avert abuses. Clear guidelines are necessary to ensure that grounds of national security are only invoked in appropriate, adequately reviewed cases. The Global Principles, in my view, provide a well thought-out, balanced set of guidelines in this respect. They stress those issues of particular, legitimate public interest which should not be classified as secret. Especially information pertaining to serious human rights violations

---

Mr Bucur worked in the telephone communication monitoring department in a military unit of the SRI (the Romanian intelligence service) based in Bucharest. Relying on Article 10 (freedom of expression), Mr Bucur successfully complained about his criminal conviction for divulging information classified "top secret". He had released audio cassettes at a press conference containing recordings of the telephone calls of several journalists and politicians, together with incriminating elements he had noted down in the register of conversations.

– *Guja v. Moldova* (2008), Application No. 14277/04

The government's dismissal of a public prosecutor for making unauthorised disclosures (concerning undue political pressures on the judiciary) to a newspaper constituted an unlawful interference with his freedom of expression (right to impart information) as it was not necessary in a democratic society.

135. Ibid., Principle 39.A.

136. Ibid., Principle 39.B.

137. Ibid., Principle 41.E; see, in this connection, although not concerned with the national security exemption, the controversy in the United Kingdom over "gagging clauses" signed by staff in the National Health Service (www.bbc.co.uk/news/health-21780425).

138. Ibid., Principle 42.C.

139. Ibid., Principle 42.

committed by public officials should never be classified as secret. A possible embarrassment for the government of the day is not a threat to national security. Agencies dealing with national security issues should be regularly monitored, including by dedicated, robustly mandated, well-resourced parliamentary or judicial oversight bodies, and last but not least, whistle-blowers should enjoy adequate protection.

98. The Parliamentary Assembly's role in promoting the effective protection of human rights in the Council of Europe's member States implies that it should actively participate in developing and promoting common standards on the right of access to information whilst respecting legitimate national security concerns, as I have done in this report, in co-operation with the Global Principles project facilitated by the Open Society Justice Initiative. We should now urge national parliaments to establish effective oversight bodies to ensure that those standards are fulfilled. We should also see to it that European institutions (including the Council of Europe and the European Union) set positive examples in this respect and grant the widest possible access to the information held by them.

99. In the draft resolution, I have summed up the main considerations that we should all be able to agree upon. I am also proposing a draft recommendation to the Committee of Ministers, for the purpose of enlisting our member States' governments in our efforts to breathe life into the Council of Europe Convention on Access to Official Documents.