

DRAFT

**PRINCIPLES ON
NATIONAL SECURITY AND THE RIGHT TO INFORMATION**

Draft September 22, 2011

Introduction.....	1
Preamble	3
Part I: General Principles	5
Part II: Information that legitimately may be withheld on national security grounds, and information that should be disclosed	9
Part IIIA: Rules regarding classification and declassification of information.....	11
Part IIIB: Rules regarding handling of requests for information	14
Part IV: Judicial oversight	16
Part V: Bodies that oversee security sector oversight institutions and information	19
Part VI: Protection of personnel who disclose information.....	22
Part VII: Limits on measures to punish or restrain the disclosure of information to the public	26
Part VIII: Concluding principles.....	28
Annex: Categories of information with a high presumption in favour of disclosure	Error!

Bookmark not defined.

INTRODUCTION

These Principles are being drafted in order to provide guidance to people engaged in drafting, revising or implementing laws or provisions relating to the government’s authority to withhold information on national security grounds or to penalize the publication of such information.

They are based on international and regional law and standards, evolving state practice, the general principles of law recognized by the community of nations, and the writings of experts.

These Principles address national security rather than all grounds for withholding information in order to start the process of developing consensus concerning the parameters of permissible restrictions on public grounds. Addressing all grounds would require more time and resources than we have, and would result in an even longer set of Principles. Moreover, national security is the weightiest public ground for restricting information so that all other public grounds for restricting access must at least meet these standards.

These Principles have been drafted, and continue to be reviewed and revised, by experts, including at meetings held around the world, in consultation with the four special mandates on freedom of expression –

- the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression,
- the Organisation for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media,
- the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression, and

- the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information –

and in collaboration with the following 14 non-governmental organizations and academic centres:¹

- Open Society Justice Initiative (global)
- Article 19, the Global Campaign for Free Expression (global);
- Africa Freedom of Information Centre (Kampala/ Africa);
- Centre for Applied Legal Studies, Witwatersrand University (Johannesburg/ South Africa);
- Centre for Democratic Control of the Armed Forces (Geneva/ global);
- Centre for Law & Democracy (global);
- Centre for National Security Studies (Washington, DC/ US and Europe);
- Centre for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law (Buenos Aires/ Latin America);
- Commonwealth Human Rights Initiative (New Delhi/ Commonwealth);
- Conectas Direitos Humanos (São Paulo/ global south);
- Egyptian Initiative for Personal Rights (Cairo/ Egypt);
- Institute for Security Studies (Africa);
- International Commission of Jurists (Geneva/ global); and
- National Security Archive (Washington, DC/ global).

Background and Rationale

No questions are more important to ensuring democratic government and fundamental human rights than those involving decisions about war, peace and protection of a country's national security. Inherent in this truism, however, is a fundamental tension. On the one hand, democracy and respect for fundamental human rights depend on public access to government information: access to information not only safeguards against abuse by governments, officials and private entities working with them, but also permits citizens to play a role in determining the policies of their governments. On the other hand, the conduct of diplomacy, military operations and intelligence activities all require some measure of secrecy in order to be effective.

Striking the right balance is made all the more challenging by the fact that courts in most 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 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.

¹ Each organisation is followed by the name of the city where headquartered – unless the organisation has substantial operations in three or more cities – and its geographic area of operation.

We, the above named organisations, undertook to elaborate these Principles to respond to the above-described long-standing challenges as well as to the fact that, in recent years, a significant number of countries around the world have embarked on adopting or revising classification regimes and related laws. This trend in turn has been impelled by at least three developments. First, the more than 70 countries -- including the population giants of China, India, Indonesia and Russia -- that adopted access to information laws since the fall of the Berlin Wall, are for the first time grappling with how to keep information secret pursuant to law, whereas previously decisions as to whether to disclose information were completely discretionary.² Second, the war on terror has provided an impetus for many governments to enhance their secrecy regimes and increase secret surveillance. Third, and relatedly, NATO issued a new information policy in 2002 that requires member states and states seeking membership to institutionalise and tighten their systems for handling national security information.³

PREAMBLE

The organizations and individuals involved in drafting the present Principles:

Reaffirming their conviction that both the right to information and the ability of the government to maintain legitimate secrets are vital to a democratic society, and are essential for its security, its progress and welfare, and the full enjoyment of human rights and fundamental freedoms;

Recognizing that it is imperative, if people are to be able to monitor the conduct of their government and to participate fully in a democratic society, that they have access to information held by public authorities, including information that relates to national security;

Bearing in mind relevant provisions of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples' Rights, the Declaration of Principles on Freedom of Expression in Africa,⁴ the American Convention on Human Rights, the Model Inter-American Law on Access to Information,⁵ the European Convention on Human Rights, and the Council of Europe Convention on Access to Official Documents;

Recalling the 2004 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media; and the Inter-American Commission on Human Rights Special Rapporteur on Freedom of Expression; the 2006, 2008, 2009 and 2010 Joint Declarations of those three experts plus the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information;

² As of August 2011, more than 85 countries had national laws or judicially enforceable regulations conferring the right of access to information, at least in law, to more than 4.5 billion people.

³ Security Within the North Atlantic Treaty Organisation, Doc. C-M(2002)49, adopted 26 March 2002, issued 17 June 2002, including Enclosure E on Security of Information and Enclosure F on INFOSEC, as revised by the Directive on Security of Information, Doc. AC/35-D/2002-Rev2, issued 4 Feb 2005.

⁴ *Declaration*, Issued by the African Commission on Human and Peoples' Rights, 32nd Session, 17 - 23 October, 2002: Banjul, The Gambia.

⁵ The General Assembly of the Organisation of American States, at its June 2010 session, adopted a resolution, to which the Model Law is appended, offering to provide support to member States with the design and execution of their regulations and policies on access to information. AG/RES 2607 (XL-0/10). See http://www.oas.org/dil/access_to_information_model_law.htm .

and the December 2010 Joint Statement on WikiLeaks of the UN and Inter-American Special Rapporteurs;

Further recalling the [Johannesburg Principles on National Security, Freedom of Expression and Access to Information](#) adopted by a group of experts convened by Article 19 in 1995,⁶ the [Principles of Oversight and Accountability for Security Services in a Constitutional Democracy](#) elaborated in 1997 by the Centre for National Security Studies (CNSS) and the Polish Helsinki Foundation for Human Rights, and the “[good practices on legal and institutional frameworks for intelligence services and their oversight](#)” issued in 2010 by Martin Scheinin, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.⁷

Noting that these Principles do not address substantive standards for intelligence collection, management of personal data, or intelligence sharing, all of which are ably addressed by Mr. Scheinin’s “Good Practices”;

Further noting that these Principles are based on international and regional law and standards relating to the right of access to information held by public authorities and other human rights, evolving state practice (as reflected, *inter alia*, in judgments of international and national courts and tribunals), the general principles of law recognized by the community of nations, and the writings of experts;

Emphasizing the need for protection of the right to public information by laws drafted with precision, and with narrowly drawn exceptions, and for oversight of the right by independent courts, parliamentary bodies and other autonomous institutions;

Further recognizing that barriers to public and independent oversight created in the name of national security increase the risk that illegal, corrupt and fraudulent behaviour may occur and may not be uncovered; and that violations of privacy and other individual rights often occur under the cloak of national security secrecy;

Concerned by the costs to national security of over-classification, including the hindering of information-sharing among government agencies and allies, the inability to protect legitimate secrets, the inability to find important information amidst the clutter, repetitive collection of information by multiple agencies, and the overburdening of security managers;

Desiring to promote robust protection of both the public’s right to information and the need to keep some information secret as fundamental elements of national security;

Further desiring to provide practical guidance to governments, legislative and regulatory bodies, public authorities, drafters of legislation, the courts, other oversight bodies, and civil society concerning some of the most challenging issues concerning the intersection of national security and the right to national security information, especially those that impact respect for human rights and democratic accountability;

Acknowledging that information that should not be classified on national security grounds may nonetheless be withheld on various other grounds recognized in international law –

⁶ See *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information* [hereinafter “Jo’burg Princs”].

⁷ Martin Scheinin, “Good Practices,” UN Doc. No. A/HRC/14/46, issued 17 May 2010.

including, e.g., international relations, fairness of judicial proceedings, rights of litigants, and personal privacy - subject always to the principle that information may not be withheld where the public interest in access to the information outweighs the public interest in maintaining the information's secrecy;

Endeavouring to elaborate Principles that are of universal value and applicability;

Recognizing that states face widely varying challenges in balancing public interests in disclosure and secrecy of national security information, and that implementation of these Principles must take into consideration local realities – including diverse legal systems, cultures, traditions and developmental circumstances;

Recommend that appropriate bodies at the national, regional and international levels undertake steps to disseminate and discuss these Principles, and endorse, adopt and/or implement them to the extent possible, with a view to achieving progressively the full realization of the right to information as set forth in Principle 1:

PART I: GENERAL PRINCIPLES

Principle 1: Right to Information

- (a) Everyone has the right to seek, receive, re-use and impart information held by or on behalf of public authorities, or to which public authorities are entitled by law to have access, including information relating to national security matters.
- (b) Public authorities are obliged to make information available on request, and have an affirmative obligation to publish information of public interest, including about national security matters, subject only to limited exceptions in law necessary to prevent specific, identifiable harm to legitimate interests.

*Definitions: "Public authorities" include all bodies within the executive, legislative and judicial branches at all levels of government, constitutional and statutory authorities, and non-state bodies that are owned or controlled by government or that serve as agents of the government. Public authorities also include private or other entities that perform public functions or services or operate with substantial public funds or benefits; these principles are applicable to information held by these entities concerning their public functions, services, or use of public funds or benefits.*⁸

"Information" refers to any type of material that communicates something and is held in any form, including 'documents' (i.e. physical material containing information, such as a report, computer file or video), and content relating to a subject, such as statistical data or discussion about a certain policy issue.

⁸ See, e.g., Model Inter-American Law on Access to Information, OAS Gen Assembly RES. 2607 (XL-O/10), adopted at the fourth plenary session, June 8, 2010, Art. 3. The Draft General Comment No. 34 on Article 19 of the International Covenant on Civil and Political Rights similarly states that "Public bodies include all levels of State bodies and organs, including the judiciary, and with regard to the carrying out of public functions, it may include other bodies." (para. 18.) This language of the draft General Comment has gone through a second reading and is likely to be adopted without changes by the UN Human Rights Committee by the end of 2011.

“Information of public interest” is information that is of serious concern or benefit to the public, not merely of individual interest. The question is not whether information is “of interest to the public” but whether disclosure is “in the interest of the public,” for instance, because it is useful for public understanding of government activities.⁹

Principle 2: Application of these Principles

These principles apply to information held by a public authority where the authority asserts that the release of such information could cause harm to national security, defence, intelligence activities or international relations of the state.

Given that national security is the weightiest public ground for restricting information, all other public grounds for restricting access must at least meet these standards.

Note: What constitutes national security varies from state to state. In most countries, defence against external threats lies at the core of the concept. In some countries, the term refers to interests primarily defended by the intelligence services. In a few countries, the definition encompasses international relations concerning core national interests. By asserting that the Principles apply to information concerning defence, intelligence and international relations, this Principle does not suggest that these concepts should be included within a definition of national security interests, but only that these concepts are sufficiently inter-related in practice that these Principles should apply in all instances when governments invoke these concepts to restrict access to information.

Principle 3: Requirements for Restricting the Right to Information on National Security Grounds

The right to information concerning national security matters may be restricted only if the following conditions are met:

- (a) the constitution or a law defines national security precisely, indicates the criteria to be used in determining whether or not information may be declared secret, and sets forth clear and narrow categories of information that may be withheld on national security grounds with sufficient precision to enable persons to understand what information may be withheld and what should be disclosed;¹⁰
- (b) disclosure of the information poses an identifiable and significant risk of irreparable harm to a legitimate and compelling national security interest in a democratic society consistent with international law;
- (c) the restriction is necessary and proportionate in a democratic society, meaning that the harm from disclosure [clearly] [greatly] outweighs the overall public interest in disclosure of the

⁹ See judicial decisions, including of the UK and Australia. [Need to look for definitions from various regional and national bodies.]

¹⁰ See 2004 Joint Declaration by UN 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, at <http://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.

information, the restriction is the least restrictive means available to protect against the harm, and the restriction does not impair the very essence of the right to information;

- (d) the restriction does not, by its terms or in the manner applied, discriminate against requesters on the basis of their characteristics or status;¹¹
- (e) the law provides for adequate safeguards against abuse, including prompt full and effective scrutiny of the validity of the restriction by independent oversight authorities, including a court.

Note to (a): A restriction is not legitimate if, for instance, its primary purpose is to protect the personal interests of those in power; prevent embarrassment; conceal information about human rights violations or any other violation of law; shield corruption or other public wrongdoing; strengthen or perpetuate a particular political interest, party or ideology; or suppress labour unrest. While other restrictions may authorise withholding on other grounds, such as protecting specific information relevant to the nation's economy, such information should not be covered by the restrictions applicable to national security or foreign relations information.

Note to (b): In balancing the risk of harm against the public interest in disclosure, account must be taken of the possibility of mitigating any harm from disclosure through other measures, including through the reasonable expenditure of funds.

Note to (d): In a related vein, Scheinin's Good Practices offer the following comment: "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. This is important for ensuring that intelligence services confine their activities to helping to safeguard values that are enshrined in a public definition of national security."¹²

Principle 4: Burden on Public Authority to Establish Validity of any Restriction

- (a) The burden of demonstrating the validity of any restriction rests with the public authority seeking to apply it.
- (b) Any doubt should be resolved in favour of disclosure.
- (c) In discharging this burden, it is not sufficient for a public authority simply to refer to an alleged risk of harm; the authority should provide specific information, and if necessary, documentation to support its risk assessment, and any person who seeks access to the information should have an opportunity to review and challenge the asserted basis for the risk assessment.
- (d) In no case may the mere assertion, such as the issuing of a certificate, by a minister or other official to the effect that disclosure would cause harm to national security be deemed to be conclusive concerning the point for which it is made.

¹¹ These include race, colour, gender, sexual orientation, language, religion, political or other opinion, national or ethnic origin, property, birth or other status.

¹² See Scheinin's Good Practices, note to Practice 1, *supra*, note [].

Commentary: In practice, adjudicators generally defer to an agency's classification decision. This is not about changing the standard in law. Decision-making must be based on evidence. In several countries [give examples], a relevant minister or other high-ranking official may issue a certificate declaring the need for information to be classified. These Principles do not take a position on whether or not such certificates constitute a good practice. Rather, this principle emphasizes that the mere assertion that disclosure would cause harm to national security is not to be taken as conclusive as to the harm, let alone as to whether the harm outweighs the public interest in disclosure.

Principle 5: Information of Public Interest

- (a) Certain categories of information that are, or are claimed to be, related to national security are of public interest, and the public interest [clearly] outweighs any potential to harm national security. The state bears an affirmative obligation to publish such information proactively.
- (b) The state may in limited circumstances withhold information of public interest from the public or punish its disclosure. In particular, information of public interest may be withheld only if there is no reasonable means to limit the harm to a level proportionate to the public interest at stake.

Notes: A non-exhaustive list of categories of information with a high presumption in favour of disclosure is provided in Principle 10 and elaborated in Annex A.

The phrase "information of [high] public interest" has been used by regional and international human rights tribunals in finding that a restriction on the dissemination of such information and, more recently, access to such information held by public authorities, constitutes a violation of the right to freedom of expression. However, what constitutes information of "public interest" or of "high public interest" is defined only by reference to examples. [We intend to compile a list of information found to be of public interest by international and domestic courts as illustrative of the meaning of those terms as used in these Principles.]

Principle 6: No Exemption for Any Public Authority

- (a) No public authority - including the judiciary, the legislature, oversight bodies, intelligence agencies, and the office of the head of state or government - may be exempted from disclosure requirements.
- (b) Information may not be withheld simply on the ground that it was generated by a particular state, public authority or unit within an authority.

Principle 7: Access to Information by Oversight Bodies

All oversight/ombudsman/appeal bodies should have access to all information, including national security information, regardless of classification level, relevant to their ability to discharge their responsibilities.

Principle 8: Resources

States should devote adequate resources to administer these principles.

PART II: INFORMATION THAT LEGITIMATELY MAY BE WITHHELD ON NATIONAL SECURITY GROUNDS, AND INFORMATION THAT SHOULD BE DISCLOSED

Principle 9: Information That Legitimately May Be Withheld

Public authorities may restrict public access to information on national security grounds, provided that such restrictions comply with the other provisions of these Principles and the information falls within one of the following categories:

- i. Current military plans, on-going operations, and capabilities for the length of time that the information is of operational utility, to the extent that these relate to armed conflicts.

Note: The phrase “for the length of time that the information is of operational utility” is meant to require disclosure of information once the information no longer reveals anything that could be used by enemies to understand the state’s readiness, capacity, plans, etc. The phrase “to the extent that these relate to armed conflicts” is intended to exclude information related to humanitarian [interventions which do not involve armed conflict] [assistance], civil protection operations or other activities not connected to armed conflict.

- ii. Information, including technological data and inventions, about weapons, their production, capabilities or use;
- iii. Measures to safeguard critical infrastructure;
- iv. Intelligence information, including analysis collection, operations, sources and methods concerning matters that fall into one of the above categories;
- v. Information falling into one of the above categories that was supplied by a foreign state or inter-governmental body with an express and written expectation of confidentiality;
- vi. Diplomatic communications; and
- vii. Information concerning the investigation or prosecution of terrorist acts and other national security-related crimes.

Note: The point of this sub-Principle is to make clear that these Principles apply to the withholding of information concerning the investigation or prosecution of terrorist acts and other national security-related crimes, regardless of the grounds on which the information is withheld.

Principle 10: Categories of Information with a High Presumption in Favour of Disclosure

The following categories of information are subject to presumptive disclosure. Information that falls into any of these categories may be withheld only in the most exceptional circumstances, consistent with Principles 3 and 5, and only for a strictly limited period of time.

Note: Exceptional withholding may be permissible, for example, for a period that is strictly necessary to ensure the effective prosecution of national security-related offences, or to protect the dignity and rights of individuals. The categories of information listed below are set forth in greater detail in the Annex to these Principles.

A. Democratic Participation in Fundamental Decisions

1. Structures and Powers of Government

- (a) The existence of all military, police, security and intelligence authorities, and sub-units;
- (b) The laws and regulations applicable to these authorities and their oversight bodies and internal accountability mechanisms; and the names of the officials who head such authorities.
- (c) The gross overall budgets, major line items and basic expenditure information by such authorities.
- (d) The existence and terms of concluded bilateral and multilateral agreements, and other major international commitments by the state on national security matters.

2. Important Decisions or Policies, including Decisions to Commit Combat Troops Overseas

- (a) Information that shows that the Government has mischaracterized a fact relevant to an important decision or policy
- (b) [More...]

3. Surveillance

- (a) The laws and primary regulations governing all forms of secret surveillance and systems of secret files and registers.
- (b) For persons who are being or have been subjected to unlawful surveillance, notification of that fact and/or recourse to review of their claims by an independent authority.

4. Detention and Interrogation

- (a) Laws, regulations [and policies] concerning detention, cross-border transfers of detainees, treatment of detainees, including methods and means of interrogation by, or [on behalf of] [in facilitation of the conduct of], the state and its agents.
- (b) The location of all places where persons are deprived of their liberty operated by or on behalf of the state as well as the identity of, and charges against, all persons deprived of their liberty including during armed conflict.

5. Accountability concerning Security Sector Contracts and other Resources

- (a) Information concerning constitutional or statutory violations and other abuses of power, including corruption, by public authorities or officials.
- (b) Basic information regarding the integrity of security sector [procurement] [contracting], financial management of critical infrastructure, and relevant audit reports.

B. Gross Violations of Human Rights and Serious Violations of International Humanitarian Law

- (a) The names of all victims of gross violations of human rights or serious violations of international humanitarian law, including crimes under international law, committed by the State, State agents or people acting with any level of government support, whether in peace time or during an armed conflict, and the dates and circumstances of these violations; and where applicable, the location of mortal remains.
- (b) The names of units and their superiors and commanders present at the time of, or otherwise implicated in, such human rights or international humanitarian law violations.
- (c) Other information concerning gross violations of human rights or serious violations of international humanitarian law committed by agents of the State that holds the information or by other States.

C. Public Health, Safety and the Environment [*To be further developed*]

- (a) Emergency response plans.
- (b) Pollution and emissions.

PART IIIA: RULES REGARDING CLASSIFICATION AND DECLASSIFICATION OF INFORMATION

Principle 11: Purpose of Classification

- (a) The purpose of a system of classification is to provide guidance to those who are involved in classifying information or have access to classified information about how the information should be classified, declassified and handled within and among public authorities.
- (b) There is no duty to classify, but there is a duty for public authorities to state reasons for withholding information.

Principle 12: Marking and Justification Requirements

- (a) When a record is classified, (i) a protective marking should be affixed indicating the level and maximum duration of classification, and (ii) a statement should be included justifying the need to classify at that level and for that period.
- (b) The justification should indicate the category of information listed in Principle 9 - or the relevant equivalent in national law, which may use different but not more expansive categories - to which the information belongs and describe the harm that could result from disclosure, including its level of seriousness and degree of likelihood.
- (c) Classification levels, if used, should correspond to the levels and likelihood of harm identified in the justification.

Note: Procedures for classifying documents vary from country to country. Paragraph-by-paragraph marking is accepted practice in some countries and is considered too onerous in others. In some countries where there was strong initial resistance, practices have been developed that lessen the administrative burden and compliance has become the rule.

For instance, several governments have developed guides that include lists of justifications, so that only a number needs to be written or linked to the classification level.

Providing a statement justifying each classification decision is encouraged because it makes officials advert seriously to the specific harm that would result from disclosure, and because it facilitates the process of declassification and disclosure. Paragraph by paragraph marking further facilitates consistency in disclosure of unclassified portions of documents.

Principle 13: Public Access to Classification Rules

- (a) The public should have access to the written procedures and standards governing classification or other withholding.
- (b) The public should have the opportunity to comment on the procedures and standards governing classification prior to their entry into force.

Principle 14: Authority to Classify

- (a) Only officials specifically authorized or designated [by the head of a public authority] may classify information. If an undesignated official believes that information must be classified, the information may be withheld for a brief and expressly defined period of time until a designated official has reviewed the recommendation for classification.
- (b) The identity of the person responsible for a classification decision should be traceable and [indicated on the document] so as to ensure accountability and to enable readers to determine the context of the decision.
- (c) Heads of public authorities should assign original classification authority to the smallest number of senior subordinates that is administratively efficient.

Principle 15: Facilitating Internal Challenges to Classification or Withholding of Information

Public personnel, especially those affiliated with security sector authorities as defined in Principle 34, who believe that information has been improperly classified or otherwise withheld should be encouraged to challenge the classification or withholding of the information.

Principle 16: Duty to Make an Index of Classified Information

Each public body shall create, and update annually, a detailed list of the classified records it holds, save for those exceptional documents whose very existence is legitimately classified in accordance with Principle 21. This list shall not be deemed to be confidential.

Principle 17: Duty to Archive and Maintain Properly National Security Information and Documents

- (a) The state and its employees have a duty to preserve and archive documents and information according to international professional standards.¹³ Documents and information may be exempted from preservation and archiving only according to law.
- (b) Information should be maintained properly. Filing systems must be consistent, transparent (without revealing classified information), and comprehensive, so that reasonably specific requests for access will locate all relevant information even if the information cannot be declassified.

Principle 18: Time Limits for Period of Classification

- (a) Information may be withheld on national security grounds for only as long as necessary to protect a legitimate national security interest. Decisions to withhold information should be reviewed periodically in order to ensure that this principle is met.
- (b) The classifier should specify the date or event (e.g., withdrawal of troops) on which the classification shall lapse.
- (c) No information shall remain classified indefinitely. The presumptive maximum period of secrecy on national security grounds must be established by law and may be extended only in exceptional circumstances.

Note: For the following reasons, a ten-year maximum period for classification is recommended for most information. [Information re international and comparative law and practice will be supplied.]

- (d) Where information is sought to be withheld beyond the presumptive deadline, the decision to do so should be made afresh and by another decision-maker, setting an amended deadline.

¹³ Current international standards for archiving are found in Charles Kecskeméti and Iván Szekelény, *Access to Archives* (Strasbourg: Council of Europe, 2005).

Principle 19: Declassification Procedures

- (a) If information of public interest, including information that falls into categories listed in Principle 10, is classified due to exceptional sensitivity, it should be declassified as rapidly as possible. Procedures should be put in place to identify classified information of public interest for priority declassification.
- (b) National legislation should specify procedures for en bloc (bulk and/or sampling) declassification.
- (c) National legislation should identify fixed periods for automatic declassification for different categories of classified information. To minimize the burden of declassification, records should be automatically declassified without review wherever possible.
- (d) National legislation should set out an accessible and public procedure for requesting declassification of documents.
- (e) Declassified documents, including those disclosed publicly by oversight/ombudsman/appeal bodies, should be proactively disclosed or otherwise made publicly accessible (for instance through harmonization with national archives legislation or access to information legislation or both).

Note: Additional good practices include the following:

- *identification in law of government responsibility to coordinate, oversee, and implement government declassification activities, including consolidating and regularly updating declassification guidance.*
- *regular consideration of the use of new technologies in the processes of declassification.*
- *regular consultation with persons with professional expertise concerning the process for establishing declassification priorities, including both automatic and en bloc declassification.*

PART IIIB: RULES REGARDING HANDLING OF REQUESTS FOR INFORMATION

Principle 20: Duty to Consider Request Even if Information Has Been Classified

The fact that information has been classified is not decisive in determining how to respond to a request for that information. Rather, the public authority that holds the information should consider the request according to these Principles.

Principle 21: Duty to Confirm or Deny

- (a) Upon receipt of a request for information, a public authority must confirm or deny whether it holds the requested information, except in extraordinary circumstances in which the very existence or non-existence of the information may be kept secret in accordance with Principle 3.

- (b) Any refusal to confirm or deny the existence of information, in context of a particular request, must be based upon a distinct information category recognized as holding such exceptional sensitivity.

Principle 22: Duty to State Reasons for Denial in Writing

- (a) If a public authority denies a request for information, in whole or in part, it must set forth in writing specific reasons for doing so as soon as reasonably possible.
- (b) The authority should also inform the requester of the identity of the official who authorized non-disclosure unless to do so would itself disclose restricted information, and of avenues for appeal.

Principle 23: Duty to Expend Reasonable Effort to Locate Missing Information

- (a) When a public authority is unable to locate information responsive to a request, and records containing that information should have been maintained or collected, the authority should make reasonable efforts to gather the missing information for potential disclosure to the requester.¹⁴
- (b) The duty to search for information is particularly high when the information concerns gross human rights violations.¹⁵

Principle 24: Duty to Disclose Parts of Documents

Exemptions from disclosure apply only to specific information and not to whole documents or other records. Only specific information for which the validity of a restriction has been demonstrated (“exempt information”) may be withheld. Where a record contains both exempt and non-exempt information, public authorities have an obligation to segregate and disclose the non-exempt information if those portions are reasonably segregable.

Principle 25: Duty to Identify Information Withheld

A public authority that holds information that it refuses to release should identify such information with as much specificity as possible. At the least, the authority should disclose the amount of information it refuses to disclose, for instance by estimating the number of pages.

Principle 26: Duty to Provide Information in Available Formats

Public authorities should provide information in the format preferred by the requester to the extent possible and, at the least, should make information available in all formats that they have or into which the information can readily be transformed.

¹⁴ This Principle is set forth in the Model Inter-American Access to Information Law, *supra* note [], Principle 33.

¹⁵ See Inter-American Court of Human Rights, judgment in *Gomes Lund v. Brazil (Araguaia Guerrilla case)*, paras __.

Principle 27: Time Limits for Responding to Information Requests

- (a) Time limits for responding to requests, including on the merits, internal review, decision by an autonomous body if available, and judicial review should be established by law and should be as short as practicably possible.
- (b) Expedited time limits should apply where there is a demonstrated public need for the information on an urgent basis.
- (c) Time limits should take into account the volume of documents requested. If volume is slight, a shorter period than the statutory deadline is likely to be practicably possible; if volume is great, an extension of time may be appropriate.

Note: It is considered a best practice, in keeping with the requirements set forth in most access to information laws, to prescribe twenty working days or less as the time period in which a substantive response must be given. See www.right2info.org/laws.

Principle 28: Right to Review of Decision Refusing Information

- (a) A requester has the right to a speedy and low cost or free review of a refusal to disclose information, including of an implicit or silent refusal, or of related matters, including fees, timelines, format, etc., by a administrative authority independent of the authority that denied the information request, as well as by a court.
- (b) The reviewing public authority must have full access to all relevant information.

PART IV: JUDICIAL OVERSIGHT

Principle 29: General Judicial Oversight Principle

- (a) National security may not undermine the fundamental right to a fair trial.
- (b) Where a public authority seeks to withhold information on the grounds of national security in any legal proceeding, a court should be permitted to, and ordinarily should, examine the information.

Note: It is good practice that the court should not rely on summaries or affidavits asserting the need for secrecy. In some cases, the judge who decides the issues regarding disclosure may not be the same judge who decides the merits of a case. For instance, under German law, a merits judge may not have access to information that the parties do not have.

- (c) No court should take as conclusive to the request for non-disclosure of information the fact that a document has been classified.
- (d) The court should adjudicate the legality and appropriateness of the public authority's claims, both substantively and procedurally, and may compel disclosure or order appropriate relief in the event of partial or full non-disclosure, including the dismissal of charges in criminal proceedings.

- (e) The court should independently assess whether the public authority has properly invoked any claimed privilege or other basis for non-disclosure, the nature of any harm claimed by the public authority and its likelihood of occurrence. Similarly, the court should assess the public interest in disclosure, the impact on the rule of law and international human rights obligations of non-disclosure and the right to a remedy claimed by either party.
- (f) Where a court rules that information has been properly withheld, it should provide fact-specific reasons and its legal analysis in writing. These reasons should be public, except in extraordinary circumstances. In such extraordinary circumstances, the public authority should make publicly available as much information as possible, including access to the legal reasoning supporting the decision.

Principle 30: Judicial Oversight of Denials of Information

A person who is refused access to information following a request for information in either an administrative or judicial process is entitled to judicial review of the denial, and also of related matters, including fees, timelines, format, etc. This should include *de novo* review of the legal issues and factual findings.

Principle 31: Public Access to Judicial Processes

- (a) National security concerns may not undermine the fundamental right of the public to access judicial processes.
- (b) Court judgments should be made public.¹⁶
- (c) Unless strictly necessary and in compliance with these Principles, the public’s right of access to judicial proceedings should include public access to (i) judicial reasoning; (ii) information about the existence and progress of cases; (iii) court hearings and trials¹⁷; and (iv) evidence in court proceedings that forms the basis of a conviction.
- (d) The public should have an opportunity to contest any claim asserted by the public authority that a restriction on judicial openness is strictly necessary on national security grounds. This includes the partial or complete closure of a hearing, the sealing of records, the non-disclosure of evidence, the redaction of a judicial opinion, or any other restriction.

Note: This Principle is not intended to modify a nation’s existing law regarding preliminary procedures to which the public does not ordinarily have access. It applies only when the court process would otherwise allow public access and the attempt to deny that access is based on a claim of national security. The public’s right of access to court proceedings and materials derives from the significance of access to promoting (i) the actual and perceived

¹⁶ International law permits no derogation on national security grounds from the obligation to pronounce judgments publicly. See, e.g., ECHR, Art. 6.1. Under the ICCPR, the only limited exception permitted for public judgment is “where the interest of juvenile persons otherwise requires or the proceedings concern matrimonial disputes or the guardianship of children.” ICCPR, Art. 14.1.

¹⁷ In the case of public access to hearings, article 14(1) of the ICCPR and article 6(1) of the ECHR reflect the authority of the courts to exclude all or part of the public from a hearing for reasons of morals, public order, national security in a democratic society, the interest of the private lives of the parties, or to avoid prejudice to the interests of justice, provided that such restrictions are in all cases necessary and proportional. See Principle 3.

fairness and impartiality of judicial proceedings; (ii) the proper and more honest conduct of the parties; and (iii) the enhanced accuracy of public comment.

Commentary to (c)(iv): Where cases are tried before a jury, all evidence that the jury considers should be public because it is not possible to know on what evidence the jury relied in deciding to convict. Where the trier of fact is a judge, if the judge expressly states that s/he did not rely on secret evidence in reaching a verdict, then that evidence need not be made public.

Principle 32: Party Access to Information in Criminal Proceedings

- (a) The court may not prohibit a defendant from attending his or her trial on national security grounds.
- (b) In no case should a conviction be based on evidence that the accused has not had an opportunity to review and refute.
- (c) In no case may a public authority fail to disclose the charges against a person.
- (d) The public authority must disclose the charges, any information it intends to use against a defendant, any potentially exculpatory evidence and any information that may assist the defendant in obtaining a reduction in sentence to the court hearing the case, the defendant's counsel, and the defendant to the extent required by criminal law without regard to the fact that information is classified subject to the limitations provided for in (e) and (f).

Commentary: Exculpatory evidence includes not only material establishing innocence but also other evidence that could assist the defence, such as indications that a confession was not voluntary or information which may assist the accused in obtaining a reduction in sentence.

- (e) Any decision to restrict or withhold the disclosure of information on national security grounds that would otherwise be required to be disclosed to a defendant must be strictly necessary and sufficiently counterbalanced by the court to enable the defendant to have substantially the same ability to respond to the charges as s/he would have had if s/he she had access to the information.
- (f) Where the public authority declines to disclose information identified in (d), above, and it is not possible to substitute information that can be disclosed and that does not prejudice the defendant's rights, the court must dismiss the charges.

Note: The public authorities cannot rely on information to their benefit when claiming secrecy, although they may decide to keep it secret and suffer the consequences. [Outline the more complex consequences of claims of secrecy vis-à-vis information of benefit to the third party here or elsewhere.]

Principle 33: Party Access to Information in Civil Cases

- (a) Cases Brought by Victims of Torture and Other Grave Human Rights Violations**

Victims of torture and other grave human rights violations are entitled to a remedy, including compensation for violations committed against them and public disclosure of abuses suffered. Public authorities may not withhold information material to their claims, except as consistent with Principle 10B.

(b) Other Cases

- (i) A public authority should not be able to bring a case against a person and then withhold material information on the ground of national security or related state interest. Nor should a public authority be able to withhold material information when a person makes a credible showing that the authority has committed a tort against him or her. In such cases, the court should evaluate the public authority's claim for secrecy using the strictest standard for evaluating claims under national law, and should be authorized to resolve the case in the person's favour.
- (ii) A person's claim against a public authority for breach of a contract between the public authority and the person may be considered according to the strict standard of Principle 33(b)(i), or may be reviewed with somewhat greater deference to the public authority's claims [and the knowledge of the parties when entering into the contract], consistent with national law and proportionate to the seriousness of the injury the person claims to have suffered.

PART V: BODIES THAT OVERSEE SECURITY SECTOR INSTITUTIONS AND INFORMATION¹⁸

Principle 34: Unrestricted Access to Information Necessary for Fulfilment of Mandate

- (a) States should establish, if they have not already done so, autonomous oversight bodies to oversee security sector and other agencies that keep more than *de minimis* amounts of information secret, including the operations, policy, finances and administration of such agencies.

Definitions:

For the purpose of these principles "autonomous" means institutionally and operationally independent of the executive and all security sector authorities.

"Security sector" encompasses the armed forces, police, defence ministry, and all intelligence, border control and law enforcement agencies.

Examples of oversight institutions include legislative committees, ombuds institutions, anti-corruption commissions, supreme audit institutions, and specialised non-legislative committees.

¹⁸ The Principles in this section are elaborated in detail given that the information that oversight bodies need to carry out their responsibilities often is both exempted from public disclosure and of public interest.

These principles are applicable to all bodies with oversight responsibilities related to national security, including, for example, budgetary or finance authorities that hold information concerning national defence or intelligence.

- (b) Such autonomous oversight bodies should have legally guaranteed access to all information necessary for the fulfilment of their mandates. There should be no restrictions on this access, regardless of the information's level of classification or confidentiality, upon satisfaction of reasonable security access requirements.
- (c) Information to which oversight bodies should have access includes, but is not limited to:
 - i. all records, technologies and systems in the possession of security sector authorities, regardless of form or medium and whether or not they were created by that authority;
 - ii. physical locations, objects and facilities; and
 - iii. information known by persons whom overseers deem to be relevant for their oversight functions.
- (d) Security sector and other public personnel may not be prohibited from, or punished for, furnishing oversight bodies with information.

Definition: "Public personnel" are current and former employees, conscripts, contractors and sub-contractors of public authorities, including in the security sector.

Principle 35: Powers and Resources Necessary to Ensure Access to Information

- (a) Security sector oversight bodies should have adequate legal powers in order to be able to access any relevant information that they deem necessary to fulfil their mandates.
- (b) At a minimum, these powers should include the right to question current and former members of the executive branch, employees and contractors of public authorities; request and inspect relevant records; and inspect physical locations and facilities.
- (c) Oversight bodies may also be given the powers to subpoena such persons and records and hear testimony under oath or affirmation from persons deemed to possess information that is relevant to the fulfilment of their mandates, with the full cooperation of law enforcement agencies, where required.
- (d) Oversight bodies, in handling information and compelling testimony, should take account of, *inter alia*, relevant privacy laws as well as protections against self-incrimination and other requirements of due process of law.
- (e) Oversight bodies should have access to the necessary financial, technological and human resources to enable them to identify, access and analyse information that is relevant to the effective performance of their functions, including information that is remotely located or of a highly technical character.
- (f) Security sector authorities should be required by law to afford oversight bodies the cooperation they need to access and interpret the information required for the fulfilment of their functions.

- (g) Security sector authorities should be legally required to make proactive and timely disclosures to oversight bodies of specific categories of information that overseers have determined are necessary for the fulfilment of their mandates. Such information should include, but not be limited to possible violations of the law and human rights standards.

Principle 36: Transparency of Security Sector Oversight Bodies

A. Applicability of Access to Information Laws

Laws that entitle members of the public to access information held by public authorities should apply to security sector oversight bodies, including legislative committees.

B. Reporting

- (a) Oversight bodies should be legally required to produce periodic reports and to make these reports publicly available. These reports should include, at a minimum:
 - i. Information on the oversight body itself, including membership, budget, performance and activities; and
 - ii. Information on those aspects of security sector authorities that fall under the oversight body's mandate.
- (b) Oversight bodies should also provide public versions of their thematic and case-specific studies and investigations, and should disclose as much information as possible concerning matters of public interest, including those areas listed in Principle 10.
- (c) Oversight bodies should respect privacy rights of all individuals concerned.
- (d) Overseers should give security authorities and the executive the opportunity to review, in a timely manner, any reports which are to be made public in order to allow them to raise concerns about the inclusion of material that may be classified. The final decision regarding what should be published should rest with the oversight body itself.

C. Outreach and Accessibility

- (a) The legal basis for oversight bodies, including their mandates and powers, should be publicly available and easily accessible.
- (b) Oversight bodies should create mechanisms and facilities for people who are illiterate, speak minority languages, or are visually or aurally impaired.
- (c) Oversight bodies should provide a range of freely available mechanisms through which the public (including those in geographically remote locations) can make contact with them and, in the case of complaints handling bodies, file complaints or register concerns, including mechanisms that can effectively preserve the confidentiality of the complaints and the anonymity of the complainant.

Principle 37: Protection of Information Handled by Security Sector Oversight Bodies

- (a) Oversight bodies should be required by law to implement all necessary measures to protect information in their possession.
- (b) [Legislatures should decide whether (i) members of legislative oversight committees, and (ii) heads and members of autonomous, non-legislative oversight bodies should be subject to security vetting prior to their appointment.]
- (c) Staff members of security sector oversight bodies should be subject to the same vetting procedures as members of the authorities they oversee. Such vetting should be conducted in a timely manner.
- (d) Oversight bodies should take the final decision on whether or not to grant a security clearance to members.
- (e) Subject to the Principles in Parts VI and VII, members or staffers of oversight bodies who disclose classified or otherwise confidential material outside of the body's normal and legally defined reporting mechanisms should be subject to appropriate administrative, civil or criminal proceedings.

Principle 38: Authority of the Legislature to Make Information Public

The legislature should have the power to disclose information to the public if it deems it appropriate to do so according to procedures that it should establish.

PART VI: PROTECTION OF PUBLIC PERSONNEL WHO DISCLOSE INFORMATION

Principle 39: Duty to Disclose Internally or to Oversight Bodies Information Showing Wrongdoing

Public, including security sector, personnel should have a duty to disclose internally or to an oversight body information relating to the following non-discrete categories of wrongdoing:

- i. significant violations of the law, including human rights violations;
- ii. significant mismanagement;
- iii. conflicts of interest;
- iv. corruption;
- v. abuse of public office; and
- vi. dangers to public health, safety and the environment.

These shall be “protected” disclosures if they comply with conditions set forth in Principles 40 and 44.

Principle 40: Protection from Penalties for Disclosures of Information Showing Wrongdoing Internally or to Oversight Bodies

- (a) The law should not impose penalties on public personnel who make protected disclosures of information internally or to oversight bodies, whether or not the information is classified or otherwise confidential, so long as at the time the disclosure was made, the person making the disclosure had reasonable grounds to believe that the information (i) was true and (ii) related to one of the categories of wrongdoing set forth in Principle 39.
- (b) The motivation for a protected disclosure is irrelevant so long as the disclosure is neither frivolous nor vexatious.
- (c) A person making a protected disclosure should not be required to bear the burden of proof, produce supporting evidence or supply his or her name. Oversight bodies should consider anonymous protected disclosures on their merits.

Note: Where a protected disclosure is unsupported by evidence, the oversight body should undertake an investigation but ultimately may not be able to take any action.

Principle 41: Procedures for Making and Responding to Protected Disclosures Internally

- (a) The law should require public security sector authorities to establish internal procedures for receiving protected disclosures of information showing wrongdoing, and investigating and resolving the matters raised.
- (b) The investigation should be as free from unnecessary administrative impediments as possible.
- (c) The public authority should be required to inform a complainant of the complainant's right to complain to an autonomous body.

Principle 42: Procedures for Making and Responding to Protected Disclosures to Autonomous Bodies

- (a) States should establish or identify autonomous, statutorily created bodies to receive protected disclosures of information showing wrongdoing, and investigate and resolve the matters raised if they are not investigated and resolved through other mechanisms or processes.
- (b) These bodies should be institutionally and operationally independent from all of the security sector and other authorities from which disclosures may be made.
- (c) The law should guarantee their access to all relevant information and afford them the necessary investigatory powers to ensure this access. Such powers may include subpoena powers and the power to require that testimony is given under oath or affirmation.
- (d) Such bodies should be required to establish effective measures to allow confidential submissions and to protect the anonymity of personnel who seek to make confidential submissions.

- (e) Public personnel should be able to access autonomous bodies directly.
- (f) If an autonomous body receives a protected disclosure that it is not competent to investigate it should be required to refer the information to an appropriate body in a timely manner.

Principle 43: Obligation to Investigate

Internal and autonomous oversight bodies should be obliged to investigate claims of wrongdoing that fall into one or more of the categories set forth in Principle 39.

Principle 44: Disclosures to the Media and Public at Large

Employees of public authorities may make protected disclosures, including of classified or otherwise confidential information, to the media or public at large if both of the following criteria are met:

- (a) The disclosure concerns the commission of a significant crime or concerns a matter that is of immediate and serious harm to public health, safety or the environment; and
- (b) The employee (i) has exhausted internal procedures; or (ii) has reasonable grounds to believe that disclosure through internal procedures or to an autonomous institution would be clearly impractical or could result in retaliation against him or her or any other individual.

Principle 45: Protection against Retaliation for Persons Making Protected Disclosures

A. Prohibition of Retaliation

- (a) The law should prohibit retaliation against any person who has made a protected disclosure in accordance with the procedures outlined above.
- (b) Prohibited forms of retaliation include but are not limited to:
 - i. Criminal proceedings, including but not limited to prosecution for disclosure of classified or otherwise confidential information;
 - ii. Administrative measures or punishments, including but not limited to the suspension or revocation of a security clearance; letters of reprimand; demotion; transfer; failure to promote; or termination of employment;
 - iii. Civil procedures, including but not limited to attempts to claim damages and defamation proceedings;
 - iv. Physical or emotional harassment; and
 - v. Threats of any of the above.
- (c) Action taken against individuals other than the person making the disclosure may in certain circumstances constitute retaliation.

B. Investigation of Retaliation by an Autonomous Body

- (a) A person who has made a protected disclosure has the right to report a claimed retaliation to an autonomous body.
- (b) These bodies should be required to investigate a claimed retaliation and to provide a response to the person making the report within a legally defined period of time.
- (c) These bodies should be given all necessary powers and resources to carry out their functions, including the powers to access all pertinent information and to summon relevant officials. In doing so, they should have recourse to all necessary cooperation from law enforcement authorities.

C. Remedies and Sanctions for Retaliation

- (a) The law must penalise retaliation relating to protected disclosures.
- (b) Bodies competent to receive disclosures should be empowered to require the public authority concerned to take remedial or restorative measures, including in the form of compensation and/or payment of legal fees, in response to unlawful retaliation.
- (c) These bodies should be able to penalise authorities or individuals found to have committed unlawful retaliation or recommend that another body pursues administrative, civil or criminal action.
- (d) Persons who have made a protected disclosure and claim retaliation should be entitled to appeal the findings of an autonomous body to a court.

D. Burden of Proof

If public authorities take action that would be adverse to the person making a protected disclosure, the public authority bears the burden of demonstrating that the action was unrelated to the disclosure.

Principle 46: Penalties Concerning Dissemination of Information to the Public for Persons with Authorised Access to Classified Information

- (a) The law should limit criminal penalties to, at most, the unauthorised disclosure of a clearly identified and limited category of information whose disclosure would likely cause identifiable and significant harm to national security.
- (b) Where criminal penalties exist, the law should provide for a public interest defence where:
 - i. the person acts for the purpose of disclosing serious human rights violations or significant dangers to public health or safety; and
 - ii. the public interest in the disclosure outweighs the public interest in non-disclosure.
- (c) In deciding whether the public interest in disclosure outweighs the public interest in non-disclosure, a judge or finder of fact should consider:

- i. whether the person made the disclosure through the internal procedures and/or to an autonomous body before making the disclosure to the public and, in doing so, whether the person complied with the procedures outlined in Principles 40 and 44;
- ii. whether the person had reasonable grounds to believe that the disclosure would be in the public interest;
- iii. the extent of the harm or risk of harm created by the disclosure; and
- iv. the existence of exigent circumstances justifying the disclosure.

Note: Commentary will be needed to explain variations in law and practice, evolving standards, and best practices concerning all of these issues.

Principle 47: Encouraging and Facilitating Protected Disclosures

In order to encourage and facilitate the disclosure of information showing wrongdoing, states should require all public security sector authorities to issue guidelines that give effect to the Principles in Part VI.

Note: Such guidelines should provide, at a minimum, (1) advice regarding the rights and/or duties to disclose wrongdoing, (2) the types of information that should or could be disclosed, and (3) required procedures for making such disclosures.

PART VII: LIMITS ON MEASURES TO PUNISH OR RESTRAIN THE DISCLOSURE OF INFORMATION TO THE PUBLIC

Principle 48: Protection against Penalties for Good Faith, Reasonable Disclosure by Information Officers

Persons with responsibility for responding to requests for information from the public may not be punished for releasing information that they reasonably and in good faith believed could be disclosed pursuant to law.

Principle 49: Penalties for Destruction of, or Refusal to Disclose, Information

- (a) Public personnel should be subject to penalties for wilfully destroying or tampering with information with the intent to deny the public access to it.
- (b) If a court or autonomous body has ordered information to be disclosed, and the information is not disclosed within a reasonable time, the official and/or public authority responsible for the non-disclosure should be subject to appropriate penalties, unless an appeal is filed in accordance with procedures set forth in law.

Note: The deterrent impact of penalties depends more on the likelihood that they will be imposed than on their severity. In several countries, administrative penalties, including dismissal from employment, and cancellation of pensions, have proved effective in deterring obstructive conduct when there has been a real likelihood that the penalties will be enforced.

Principle 50: Penalties Concerning Dissemination of Information by a Person without Authorized Access to Classified Information

- (a) A person may not be punished for the mere receipt or possession of classified information.
- (b) A person who does not have authorised access to classified information may not be punished for disclosing information to the public, except when disclosure actually resulted in serious harm to an individual, and the person who disclosed the information reasonably should have known that such harm was likely.
- (c) Nor may a person who does not have authorized access to classified information be subject to charges for conspiracy or other crime limited to conduct involving those with authorized access.

Notes: Third party disclosures operate as an important corrective for pervasive over-classification.

Some countries have a standard allowing for criminalisation in extremely narrow circumstances. Where this is the standard, Option B principles, below, should be met (i.e., narrowly defined statute; legitimate classification; actual, identifiable and significant harm; and harm known to result from disclosure).

OPTION B:

Persons who do not have authorized access to classified information may not be punished for disclosure to the public of information unless the government can prove that:

- i. the information was legitimately classified pursuant to national law and these Principles [and involved lawful government operations];*
- ii. the disclosure violated a narrowly drawn statute criminalizing disclosure of a clearly identified and limited category of information;*
- iii. the disclosure caused identifiable and significant harm to national security that [clearly] outweighed the public interest in publication of the information; and*
- iv. the person knew, or reasonably should have known, that such harm was likely to be caused by the disclosure.*

Principle 51: Protection of Sources

No journalist or other person who does not have authorized access to classified information may be compelled to reveal a confidential source or unpublished materials in an investigation concerning unauthorized disclosure of information to the press or public.

*Definition: The term 'journalist' refers to any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication.*¹⁹

¹⁹ See, e.g. “Recommendation No. R(2000) 7 on the right of journalists not to disclose their sources of information,” adopted by the Committee of Ministers of the Council of Europe, 8 March 2000; European Court of Human Rights, Grand Chamber judgment, *Sanoma Uitgevers B.V. v. the Netherlands*, 14 Sept 2010, para. 44.

Principle 52: Prior Restraint

- (a) Prior restraints against publication in the interest of protecting national security should be prohibited unless a court finds that the government has established that publicizing the information would surely result in irreparable harm to the nation or serious physical injury to an identifiable individual or class of individuals.
- (b) In particular, if information has been made generally available to the public, by whatever means, whether or not lawful, any effort to try to stop further publication of the information in the form in which it already is in the public domain is presumptively invalid.

Notes: Prior restraints are orders by judicial or other state bodies banning the publication of specific material.

This Principle in no way intends to encourage leaks. “Generally available” is understood to mean that the information has been sufficiently widely disseminated that there are no practical measures that could be taken that would keep the information secret. For instance, in its 1991 Spycatcher judgment, the European Court of Human Rights concluded that, once the memoirs of a retired member of the British security services had been published in the United States, a court’s permanent injunction could no longer be sustained.²⁰ With the advent of the Internet and new media tools such as GoogleEarth, not to mention sites such as WikiLeaks, previously classified or otherwise restricted information continues to enter the public domain and once there cannot easily be contained. Attempting to enjoin publication of information that has been on the Internet for any length of time would, in most circumstances, be futile, would not meet the standard for causing identifiable harm, and would tend to compromise the credibility of the classification system.

PART VIII: CONCLUDING PRINCIPLES

Principle 53: Relation of These Principles to Other Standards

Nothing in these Principles should be interpreted as restricting or limiting any right to information recognized under international, regional or national law or standards.

²⁰ The Observer and Guardian v. UK and The Sunday Times v. UK (No. 2), Judgments of 26 November 1991, Series A, No. 216 and 217, 216 Eur. Ct. H. R. (ser. A), paras. 66-70, (Observer and Guardian), and paras. 52-56 (The Sunday Times (No.2)).