DRAFT

GLOBAL PRINCIPLES ON NATIONAL SECURITY AND THE RIGHT TO INFORMATION

April 8, 2013

INTRODUCTION

These Principles were developed in order to provide guidance to those engaged in drafting, revising or implementing laws or provisions relating to the state's authority to withhold information on national security grounds or to punish the disclosure of such information.

They are based on international (including regional) and national law, standards, and [best] [good] practices, [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. All other public grounds for restricting access should at least meet these standards.

These Principles have been drafted by experts, including at [12] meetings held around the world over two years, in consultation with several partner organizations (listed in Annex A), some 500 experts from more than 60 countries, and including 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 (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information.

Background and Rationale

National security and the public's right to know are often viewed as pulling in opposite directions. While there is at times a tension between a government's desire to keep information secret on national security grounds and the public's right to information held by public authorities, 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.

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.

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 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.

These Principles respond to the above-described longstanding challenges as well as to the fact that, in recent years, a significant number of states around the world have embarked on adopting or revising classification regimes and related laws. This trend in turn has been sparked by several developments. Perhaps most significant has been the rapid adoption of access to information laws since the fall of the Berlin Wall, with the result that, as of the date that these Principles were issued, more than 5.2 billion people in 95 countries around the world enjoyed the right of access to information at least in law.[1] People in these countries are, for the first time, grappling with how to keep information secret pursuant to law rather than by culture or executive discretion. Other developments contributing to an increase in proposed secrecy legislation have been government responses to terrorism or the threat of terrorism, and an interest to having secrecy regulated by law in the context of democratic transitions.

[1] See http://www.right2info.org/laws/constitutional-provisions-laws-and-regulations.

PREAMBLE

The organizations and individuals involved in drafting the present Principles:

Recalling that access to information held by the state is a right of every person, and therefore that this right should be protected by laws drafted with precision, and with narrowly drawn exceptions, and for oversight of the right by independent courts, parliamentary oversight bodies and other independent institutions;

Recognizing that states can have a legitimate interest in withholding certain information, including on grounds of national security, and emphasizing that striking the appropriate balance between the disclosure and withholding of information is vital to a democratic society and essential for its security, progress, development and welfare, and the full enjoyment of human rights and fundamental freedoms;

Affirming 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;

Noting that these Principles are based on international and regional law and standards relating to the public's 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;

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 American Convention on Human Rights, the European Convention on Human Rights, and the Council of Europe Convention on Access to Official Documents;

Further bearing in mind the Declaration of Principles on Freedom of Expression of the Inter-American Commission of Human Rights; the Model Inter-American Law on Access to Information,[2] the Declaration of Principles on Freedom of Expression in Africa,[3] and the Model Law on Access to Information in Africa[4];

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] Doc. CP/CAJP-2840-10. The General Assembly of the Organisation of American States, at its June 2010 session, adopted a resolution, to which the Model Law is appended, noting the Model Law and 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 .

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

[4] The African Commission on Human and Peoples' Rights adopted the Model Law at its Extra-Ordinary Session in March 2013, and launched it during its April 2013 session.

the December 2010 Joint Statement on WikiLeaks of the UN and Inter-American Special Rapporteurs; and the Report on Counter-Terrorism Measures and Human Rights, adopted by the Venice Commission in 2010;[5]

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] and 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;

Noting that these Principles do not address substantive standards for intelligence collection, management of personal data, or intelligence sharing, which are addressed by the "good practices on legal and institutional frameworks for intelligence services and their oversight" issued in 2010 by Martin Scheinin, then the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, at the request of the UN Human Rights Council;[7]

Recognizing the importance of effective intelligence sharing among states, as called for by UN Security Council Resolution 1373;

Further recognizing that barriers to public and independent oversight created in the name of national security increase the risk that illegal, corrupt and fraudulent misconduct 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;

Emphasizing that the Principles focus on the *public*'s right to information, and that they address the rights to information of detainees, victims of human rights violations and others with heightened claims to information only to the extent that those rights are closely linked with the public's right to information;

Acknowledging that information that should not be classified on national security grounds may nonetheless be withheld on various other grounds recognized in international law – including, e.g., international relations, fairness of judicial proceedings, rights of litigants, and personal privacy - subject always to the principle that information may only be withheld where the national security interest in maintaining the information's secrecy clearly outweighs the public interest in access to information;

Desiring to provide practical guidance to governments, legislative and regulatory bodies, public authorities, drafters of legislation, the courts, other oversight bodies, and civil society

---

[5] Report, 4 June 2010, http://www.venice.coe.int/docs/2010/CDL-AD(2010)022-e.pdf.

[6] *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information* at http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf. *See* Coliver, et al (eds.) *Secrecy & Liberty* (Martinus Nijhoff Pubs 1999), which includes a detailed commentary on the Jo'burg Principles.

[7] Martin Scheinin, "Good Practices," UN Doc. No. A/HRC/14/46, issued 17 May 2010.

concerning some of the most challenging issues concerning the intersection of national security and the right to information, especially those that involve respect for human rights and democratic accountability;

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 the need for secrecy to protect legitimate national security interests, and that, while the Principles are universal, their application in practice may respond to local realities, including diverse legal systems;

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:

DEFINITIONS

In these Principles, unless the context otherwise requires:

"**Critical infrastructure**" – [to be defined]

"**Independent**" means institutionally and operationally independent of the executive and all security sector authorities. [More specific definition?]

"**Information**" means any original or copy of documentary material irrespective of its physical characteristics, and any other tangible or intangible material, regardless of the form or medium in which it is held. It includes, but is not limited to, records, correspondence, fact, opinion, advice, memorandum, data, statistic, book, drawing, plan, map, diagram, photograph, audio or visual record, documents, emails, logbooks, samples, models, and data held in any electronic form.[8]

"**Information of public interest**" refers to information that is of 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]

"**Judicial authority**" or "**Court**" – [to be defined with regard to independence, impartiality, effectiveness]

"**Laws**" – [definition to include decrees and orders?]

"**Public interest**" is not defined in these Principles. [An illustrative list of factors to be considered in deciding whether the public interest in disclosure outweighs the public interest in secrecy is included in a note to Principle 3(c).] [A list of categories of especially high public interest that should be published proactively and should never be withheld is set forth

[8] See definitions of information in Model Law on Access to Information in Africa, *supra* note [4]; and Model Inter-American Law on Access to Information, *supra note* [4].
[9] See [judicial decisions to be added].

in Principle 10. A list of categories of wrongdoing that are of high interest to the public, and that public servants should and may disclose without fear of retaliation, is set forth in Principle 39.]

Commentary: [Outline public interest considerations in various laws. I.e., Rwandan ATI law (2013) identifies "(1) to promote in public and private organs to which this Law applies the culture of informing the public about their activities; (2) to ensure that the expenditure of public funds is subject to effective management and oversight; (3) to promote founded public debate; (4) to keep the public regularly and adequately informed about the existence of any danger to public health or safety or to the environment; (5) to ensure that any public authority with regulatory mission properly discharges its functions."]

"**Intelligence**" – [to be defined]

["**Journalist**" refers to any natural or legal person who is regularly or professionally engaged in the collection of information and its dissemination to the public via any means of mass communication.[10]]

"**Legitimate national security interest**" refers to an interest the genuine purpose and primary impact of which is to protect national security, consistent with international and national law. Categories of information whose withholding may be necessary to protect a legitimate national security interest are set forth in Principle 9. 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.[11]

"**National security**" is not defined in these Principles. Principle 2 includes a recommendation that "national security" should be defined precisely in national law, in a manner consistent with the needs of a democratic society.[12]

"**Public authorities**" include all bodies within the executive, legislative and judicial branches at all levels of government, constitutional and statutory authorities, including security sector 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, but only in regard to the performance of those functions, provision of services or use of public funds or benefits.[13]

---

[10] 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.

[11] "Legitimate national security interest" lies at the very heart of these Principles and for that reason any positive definition will be circular. Accordingly, the term is primarily defined by what is *not* included. This is also the approach followed by the Johannesburg Principles, Principle 2.

[12] Joint Declaration 2004 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".

[13] 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 General Comment No. 34 on Article 19 of the

[OUTSTANDING ISSUE: Consideration of private bodies in the context of the principles. Suggested to consider South African law, Africa model law, Rugge principles, Arms Trade Treaty.]

"**Public personnel**" refers to current and former public employees, contractors and sub-contractors of public authorities, including in the security sector. Public personnel also includes persons employed by non-state bodies that are owned or controlled by the government or that serve as agents of the government. Public personnel also include employees of private or other entities that perform public functions or services or operate with substantial public funds or benefits, but only in regard to the performance of those functions, provision of services or use of public funds or benefits.

"**Sanction**" – [definition needed]

"**Security sector**" encompasses the [executive,]police, armed forces, defence, intelligence services, and all other law enforcement agencies.

[OUTSTANDING ISSUE: definition of security sector. Security forces as uniformed personnel; security sector broader, i.e., including oversight bodies.]

PART I: GENERAL PRINCIPLES

Principle 1: Right to Information

(a) Everyone has the right to seek, receive, use and impart information held by or on behalf of public authorities, or to which public authorities are entitled by law to have access.

(b) Public authorities are obliged to make information available on request, subject only to limited exceptions prescribed by law and necessary to prevent specific, identifiable harm to legitimate interests, including national security.

(c) Public authorities also have an affirmative obligation to proactively publish [certain] information of public interest.

Principle 2: Application of these Principles

(a) These Principles apply to the exercise of the right of access to information held by a public authority where the authority asserts that the release of such information could cause harm to national security.

(b) Given that national security is one of the weightiest public grounds for restricting information, all other public grounds for restricting access – including ~~defence, intelligence,~~ international relations, public order, public health and safety, law enforcement, future provision of free and open advice, effective policy formulation, and economic interests of

---

International Covenant on Civil and Political Rights similarly states that Public bodies are as indicated in paragraph 7 [namely, "[a]ll branches of the State (executive, legislative and judicial) and other public or governmental authorities, at whatever level – national, regional or local" and] . . . may also include other entities when such entities are carrying out public functions." (Para. 18.)

the state – must at least meet the standards for imposing restrictions on the right of access to information set forth in these Principles as relevant.

(c) It is good practice for national security to be defined precisely in the constitution or a law, [for purposes of imposing restrictions on the right of access to information], in a manner consistent with the needs of a democratic society.

Note to 2(a) and 2(b): 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 states invoke these concepts to restrict access to information.

Note to 2(c): Similarly, UN special rapporteur Martin Scheinin, in his "Good Practices" document, 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 … ."[14] *The 2004 Joint Declaration of the Rapporteurs on Freedom of Expression 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".*

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

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.

(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.[15]

(b) *Necessary in a democratic society*.

---

[14] See Scheinin's Good Practices, note to Practice 1, *supra*, note 7.

[15] 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&lID=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.

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.

Note: See definition of "legitimate national security interest." Principle 3(b) is all the more important if national security is not defined clearly in law as recommended in Principle 2.

Note to 3(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, including through the reasonable expenditure of funds. Following is an illustrative list of factors to be considered in deciding whether the public interest in disclosure outweighs the public interest in secrecy:

- *factors favouring disclosure: disclosure could reasonably be expected to (a) promote open discussion of public affairs, (b) enhance the government's accountability, (c) contribute to positive and informed debate on important issues or matters of serious interest, (d) promote effective oversight of expenditure of public funds; (e) reveal the reasons for a government decision; (f) contribute to protection of the environment; (g) reveal threats to public health or safety; or (h) reveal, or help establish accountability for, violations of human rights or international humanitarian law.*

- *factors favouring non-disclosure: disclosure would likely pose a real and identifiable risk of harm to a legitimate national security interest;*

- *factors that are irrelevant: disclosure could reasonably be expected to (a) cause embarrassment to, or a loss of confidence in, the government or an official; or (b) weaken a political party or ideology.*

The fact that disclosure could cause harm to the country's economy would be relevant in determining whether information should be withheld on that ground, but not on national security grounds.

Commentary: [To define "significant harm" in interpretation of necessity in a democratic society.]

Principle 4: Burden on Public Authority to Establish Legitimacy of Any Restriction

(a) The burden of demonstrating the legitimacy of any restriction rests with the public authority seeking to withhold information.

(b) The right to information should be interpreted and applied broadly, and any restrictions should be interpreted narrowly.

(c) In discharging this burden, it is not sufficient for a public authority simply to assert that there is a risk of harm; the authority is under a duty to provide specific substantive reasons to support its assertions.

Note [or part of principle]: Any person who seeks access to the information should have a fair opportunity to challenge the asserted basis for the risk assessment before an administrative as well as a judicial authority, consistent with Principle 28.

(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.

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 [examples will be given], 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 the issuing of such certificates constitute 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: No Exemption for Any Public Authority

(a) No public authority – including the judiciary, the legislature, oversight institutions, intelligence agencies, the armed forces, police, other security agencies, the offices of the head of state and government, or any component offices of the foregoing – may be exempted from disclosure requirements.

(b) Information may not be withheld simply on the ground that it was generated by, or shared with, a particular state, public authority or unit within an authority.

Principle 6: Access to Information by Oversight Bodies

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

Note: This Principle is expanded upon in Principle 34. It does not address disclosure to the public by oversight bodies. Oversight bodies should maintain the secrecy of all information that has been legitimately classified according to these Principles, as set forth in Principle 37.

Principle 7: Resources

States should devote adequate resources and take other necessary steps, such as the issuance of regulations and proper maintenance of archives, to ensure that these Principles are observed in practice.

Principle 8: States of Emergency

In a time of public emergency which threatens the life of the nation and the existence of which is officially and lawfully proclaimed in accordance with both national and international law, a state may derogate from its obligations regarding the right to seek, receive and impart information, only to the extent strictly required by the exigencies of the situation and only when and for so long as the derogation is not inconsistent with the state's other obligations under international law, and does not involve discrimination based on race, colour, sex, sexual orientation, language, religion, political or other opinion, national, ethnic or social origin, property, birth, disability or other similar status.

Note: Certain aspects of freedom of expression are so fundamental to the enjoyment of non-derogable rights that they should be respected even in times of national emergency.

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

(a) Public authorities may restrict the public's right of access to information on national security grounds, but only if such restrictions comply with all of the other provisions of these Principles and the information falls within one of the following categories:

i. Information about current military or security plans, on-going military or security 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.

ii. Information, including technological data and inventions, about weapons, their [production,]capabilities [or use];

Note: The acquisition of nuclear weapons [or other weapons of mass destruction] by a state, in contrast to details about their capabilities, etc.,is a matter of overriding national and global interest and should not be kept secret. This should not be read to endorse the acquisition of such weapons in any way.

iii. Information about specific measures to safeguard critical national infrastructures against external attacks or threats or use of force or sabotage;

iv. Information concerning specific measures to safeguard constitutional institutions and territory of the state against the threat or use of violence;

v. Intelligence information, including analysis collection, operations, sources and methods concerning matters that fall into one of the above categories;

Note: Methods and categories of intelligence collection should be open and subject to oversight by independent bodies.

vi. Information concerning the prevention [, investigation] [or prosecution] of terrorist attacks, subject to the rights of victims of terrorism to information about such investigations and prosecutions, and the rights of individuals subject to such proceedings to a fair and public trial and protection against violation of their human rights;

vii. Diplomatic communications insofar as they raise legitimate national security matters;

Note: "Diplomatic communications" refers to communications by diplomats of the state as well as by diplomats of other states or inter-governmental entities.

viii. Information that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality concerning legitimate national security matters; and

Note: It is good practice for such expectations to be recorded in writing.

(b) A state may add a category of information to the above list of categories provided that the category is specifically identified and preservation of the information's secrecy is necessary to protect a legitimate national security interest that is set forth in law, defined narrowly, and adopted following opportunity for public comment, as suggested in Principle 2(c). In proposing the category, the state should explain how disclosure of information in the category would harm national security.

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

Some categories of information, including those listed below, are of particularly high public interest, given their special significance to the process of democratic oversight and the rule of law. Accordingly, there is a very strong presumption, and in some cases an overriding imperative, that such information should be public and proactively disclosed.

Information in the following categories should enjoy at least a high presumption in favour of disclosure, and may be withheld on national security grounds only in the most exceptional circumstances and in a manner consistent with the other principles, only for a strictly limited period of time, only pursuant to law and only if there is no reasonable means by which to limit the harm that would be associated with disclosure. For certain subcategories of information, specified below as inherently subject to an overriding public interest in disclosure, withholding on grounds of national security can never be justified.

A. Violations of International Human Rights and Humanitarian Law

(1) There is an overriding public interest in disclosure of information regarding gross violations of human rights or serious violations of international humanitarian law, including crimes under international law, and other violations when they are perpetrated on a systematic basis; such information may not be withheld on national security grounds in any circumstances.

Note: Consistent with Principle 52, nothing in this Principle should be understood to endorse a lower standard of transparency than is required by international or national law. For example, this should not prejudice the interpretation of the laws of Brazil [Guatemala, Peru ….] that…

Commentary: [Expand upon the requirements of international law, (specifically, on the right the truth and the right to remedy, e.g. – UN and OAS sources). Gross violations includes, without limitation, torture, enforced disappearance, extrajudicial executions…"]

(2) Information regarding other violations of human rights or humanitarian law, not perpetrated on a systematic basis, is still subject to a high presumption of disclosure, and in any event may not be withheld on national security grounds in a manner that would prevent accountability for the violations or deprive a victim of access to an effective remedy.

(3) When a state is undergoing a process of transition from an [authoritarian][non-democratic] to a democratic form of government, there is always an overriding public interest in disclosure to society as a whole of all information regarding all human rights violations committed by the past regime.

OUTSTANDING ISSUE: should this be a note rather than a sub-principle? Consider un resolutions on societies in transition and post-conflict situations, right to truth, justice; IACHR right to truth cases; IACommHR (in transition, foe and ati acquire a structural importance. Indeed, on basis of these rights, can construct the past, recognize errors committed, provide remedy for victims and vigorous debate for reconstruction of rule of law and recovery); ECHR lustration cases. Noted strong concerns about perception of double standard, as well as strong concerns about importance of disclosure of information re human rights violations for the consolidation of transition. Other issues noted: economic crimes. Sub-group to follow up to include at least Ian, Catalina, Sandy Africa, Hennie, Guenter, Nevena, and Ian to consult / engage Pablo de Grieff, special rapporteur. [Matt: also technical issue.]

(4) Where the existence of violations is contested or suspected rather than already established, this Principle applies to information that, taken on its own or in conjunction with other information, would shed light on the truth about the alleged violations.

(5) This Principle applies to information about violations that have occurred, are occurring, or are likely to occur, and applies regardless of whether the violations were committed by the state that holds the information or another state.

(6) Information regarding violations covered by this principle includes, without limitation, the following:

a. A full description, including any records, of the acts or omissions that constitute the violations, as well as the dates and circumstances in which they occurred, and where applicable, the location of any missing persons or mortal remains.

b. The identities of all victims.

Note: 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 and if the withholding is consistent with human rights. Even in such circumstances, however, this should not preclude publication of aggregate or otherwise anonymous data.

c. The names of the agencies and individuals who perpetrated or were otherwise responsible for the violations, and more generally of any security sector units present at the time of, or otherwise implicated in, the violations, as well as their superiors and commanders.

d. Information on the causes of the violations and of the failure to prevent them.

B. Structures and Powers of Government

(1) [Chapeau needed?]

(2) Information covered by this principle includes, without limitation, the following:

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. Information needed for evaluating and controlling the expenditure of public funds, including the gross overall budgets, major line items and basic expenditure information for 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.

C. Decisions to Use Military Force

(1) [Chapeau needed?]

(2) Information covered by this principle includes, information relevant to a decision to commit combat troops or take other such military action, including confirmation of the fact of taking such action, its general size and scope, and an explanation of the rationale for it, as well as any information that demonstrates that a fact stated as part of the public rationale was mistaken.

Note: The reference to an action's "general" size and scope recognises that it should generally be possible to satisfy the high public interest in having access to information relevant to the decision to commit combat troops without necessarily revealing all of the details of the operational aspects of the military action in question (see Principle 9).

D. Surveillance

(1) [Chapeau needed?]

(2) Information covered by this principle includes

a. The laws and primary regulations governing all forms of secret surveillance and systems of secret files and registers.

b. [For the oversight of independent bodies, the methods and categories of intelligence collection.] [Clarify or include in note.]

Notes: Operational details of lawful surveillance may in general be withheld from individuals subject to surveillance during the period of surveillance, but the overall legal framework must set out in a form accessible to the public an indication of the procedure to be followed for authorizing the surveillance and for selecting for examination, sharing, storing and destroying intercepted material.

This principle applies equally where a state conducts surveillance through or otherwise relying upon information provided by private companies, as per Principle 2 and the definition of "public authorities".

Further, individuals who believe they have been subject to unlawful *surveillance should have access to an independent mechanism (preferably a court or tribunal) empowered to determine whether unlawful surveillance has occurred and, if so, to notify the person and provide notification of the surveillance and a description of its scope and nature.*

For persons who have been subjected to lawful *surveillance, a person should be entitled to have notification of the surveillance and a description of its scope and nature subject to [SEE AIDAN'S LANGUAGE, REFERENCE TO SCHEININ PRINCIPLES.]*

E. Safeguards for the Right to Liberty and Security of Person, the Prevention of Torture and other Ill-treatment, and the Right to Life

(1) [Chapeau needed?]

(2) Information covered by this principle includes:

(a) Laws, [decrees, orders,]regulations, and rules and policies concerning deprivation of liberty, including those that address the grounds, procedures, transfers, treatment or conditions of detention of affected persons, including methods and [means][practices] of interrogation There is an overriding public interest in disclosure of such laws, regulations, rules and policies.

Note: Deprivation of liberty includes any form of arrest, detention, imprisonment or internment.

(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, or reasons for the detention of, all persons deprived of their liberty, including during armed conflict.

(c) Laws, [decrees, orders,]regulations, rules and policies that authorize the deliberate deprivation of life of a person by the State. There is an overriding public interest in disclosure of such laws, regulations, rules and policies.

Note: This Principle should not be understood to endorse any particular such laws or regulations in any way.

(d) Information regarding the death in custody of any person, including the person's identity and the fact and cause of her or his death.

(e) Information regarding any deprivation of life for which a state is responsible, whether of a person in the custody of the state or in any other context, including the identity of the person or persons killed, the circumstances of their death, and the location of their remains.

Note to section 10E as a whole: In no circumstances may information be withheld on national security grounds that would result in the secret detention of a person, or the establishment and operation of secret places of detention, or secret executions. Nor are there any circumstances in which the fate or whereabouts of anyone deprived of liberty by, or with the authorization, support or acquiescence of, the state may be concealed from, or otherwise denied to, the person's family members or others with a legitimate interest in the person's welfare.

The names and other personal data of persons who have been deprived of liberty, who have died in custody, or whose deaths have been caused by the state, may be withheld from disclosure to the general public in order to protect the right to privacy if the person, or in the case of deceased persons, their family members, have expressly and voluntarily so requested, and if the withholding is consistent with human rights. Even in such circumstances, however, this should not preclude publication of aggregate or otherwise anonymous data.

F. Economic Crimes and Corruption

(1) [Chapeau needed?] [OUTSTANDING ISSUE: Hennie will take responsibility for reaching out to experts and consulting with working group with additional proposed language; Kate, Aidan, and Ben will discuss and propose language for public access to audit reports.]

(2) Information covered by this principle includes information sufficient for the public to assess the financial integrity of security sector finances, including procurement, [audit reports], budgets with headline items, and financial management of critical infrastructure by the security sector.

G. Accountability Concerning Constitutional and Statutory Violations and Other Abuses of Power

(1) [Chapeau needed?]

(2) Information covered by this principle includes information concerning the existence, character, and scale of constitutional or statutory violations and other abuses of power by public authorities or personnel.

G. Public Health, Public Safety or the Environment

(1) [Chapeau needed?]

(2) Information covered by this principle includes:

a. In the event of any imminent or [existing][actual] threat to public health, public safety or the environment, all information which could enable the public to 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.

b. Other regularly updated information on [the general state of the environment], 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.

PART IIIA: RULES REGARDING CLASSIFICATION AND DECLASSIFICATION OF INFORMATION

Principle 11: Duty to State Reasons for Classifying Information

(a) Whether or not a state has a formal classification process, public authorities are obliged to state reasons for classifying information.

[Note: "Classification" is the process by which records that contain sensitive information are reviewed and given a mark to indicate who may have access and how the record is to be handled. It is good practice to institute a formal system of classification, in order to reduce arbitrariness and excessive withholding.]

(b) The reasons should indicate the narrow category of information, corresponding to one of the categories listed in Principle 9, 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.

(d) When information is classified, (i) a protective marking should be affixed to the record indicating the level, if any, and maximum duration of classification, and (ii) a statement should be included justifying the need to classify at that level and for that period.

Note: Procedures for classifying documents vary from country to country. Some countries, such as the UK, do not have a formal classification system. Others, such as Mexico, do not have classification levels. 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 pay attention 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 the opportunity to comment on the procedures and standards governing classification prior to their becoming effective.

(b) The public should have access to the written procedures and standards governing classification.

Principle 14: Authority to Classify

(a) Only officials specifically authorized or designated, as defined by law, may classify information. If an undesignated official believes that information should be classified, the information may be deemed classified for a brief and expressly defined period of time until a designated official has reviewed the recommendation for classification.

Note: In the absence of legal provisions controlling the authority to classify, it is good practice to at least specify such delegation authority in a regulation.

(b) The identity of the person responsible for a classification decision should be traceable or indicated on the document, unless compelling reasons exist to withhold the identity, so as to ensure accountability.

(c) Those officials designated by law should assign original classification authority to the smallest number of senior subordinates that is administratively efficient.

Note: It is a good practice to publish information about the number of people who have authority to classify, and the number of people who have access to classified information.[16]

Principle 15: Facilitating Internal Challenges to Classification

Public personnel, including those affiliated with the security sector, who believe that information has been improperly classified can challenge the classification of the information.

Note: Security sector personnel are flagged as deserving of special encouragement given the heightened cultures of secrecy in security agencies, the fact that most countries have not

[16 See, e.g., Steven Aftergood, Federation of American Scientists, Blog, 6 Aug 2012 and US FY 2010 intelligence authorization act revealing unexpectedly high number of cleared persons eligible for access to classified information. http://www.fas.org/blog/secrecy/2012/07/cleared_population.html.]

established or designated an independent body to receive complaints from security personnel, and disclosure of security information often results in higher penalties than does disclosure of other information.

Principle 16: Duty to Make an Index of Classified Information

Each public body should create, and [biannually] [annually] [periodically] review and update, a detailed and accurate list of the classified records it holds, save for those exceptional documents[, if any,] whose very existence may legitimately be withheld in accordance with Principle 21. This list shall not be deemed to be confidential.

[Note: It is good practice to update these lists [biannually] [annually].]

[From US and Mexico practice – may be impossible. Proposals: Include within 17a as part of information management. Or keep detail in. Or include annual review.]

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 information according to international standards.[17] Information may be exempted from preservation and archiving only according to law.

(b) Information should be maintained properly. Filing systems should be consistent, transparent (without revealing legitimately classified information), and comprehensive, so that specific requests for access will locate all relevant information even if the information cannot be disclosed.

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, conditions, or event on which the classification shall lapse.

Note: A relevant event may include, e.g., withdrawal of troops. [It is good practice that this time limit, or specification of conditions or event on which classification lapses, is subjected to periodic review.]

[17] These include: "Principles of Access to Archives: a Success for Transparency and Right to Information" of the International Council on Archives (ICA), 2013, http://www.ica.org/13619/toolkits-guides-manuals-and-guidelines/principles-of-access-to-archives.html ; "Universal Declaration on Archives" of the International Council on Archives (ICA), 2010, officially endorsed by the UNESCO, http://www.ica.org/?lid=13343&bid=1101; "Recommendation No R(2000)13 on a European policy on access to archives" of the Council of Europe, https://wcd.coe.int/ViewDoc.jsp?id=366245; "Archival policies in the protection of human rights" or the so-called "Quintana report" (an updated and fuller version of the report prepared by UNESCO and the International Council on Archives (1995), concerning the management of the archives of the state security services of former repressive regimes), ICA, 2009, www.ica.org/download.php?id=971 .

(c) No information may remain classified indefinitely. The presumptive maximum period of classification on national security grounds should be established by law.

Note: For the following reasons, a 12-year maximum period for classification is recommended for most information. [Information re international and comparative law and practice will be supplied.]

(d) Information may be withheld beyond the presumptive deadline only in exceptional circumstances, pursuant to a new decision to, made by another decision-maker, and setting an amended deadline.

[Principle 18*bis*: Prohibition of Retroactive Classification

Information may not be classified after it has already been in the public domain.]

Principle 19: Declassification Procedures

(a) National legislation should identify government responsibility to coordinate, oversee, and implement government declassification activities, including consolidating and regularly updating declassification guidance.

(b) Procedures should be put in place to identify classified information of public interest for priority declassification. 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.

(c) National legislation should specify procedures for en bloc (bulk and/or sampling) declassification.

(d) 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.

(e) National legislation should set out an accessible and public procedure for requesting declassification of documents.

(f) Declassified documents, including those disclosed publicly by oversight/ombudsman/appeal bodies, including courts and tribunals, 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:

- *regular consideration of the use of new technologies in the processes of declassification; and*
- *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 should confirm or deny whether it holds the requested information.

(b) If a jurisdiction allows for the possibility that a public authority may, in extraordinary circumstances in which the very existence or non-existence of the information may be classified in accordance with Principle 3, then any refusal to confirm or deny the existence of information in response to a particular request should be based upon a showing that mere confirmation or denial of the existence of the information would pose a risk of harm to a distinct information category designated in a national law or regulation as requiring such exceptional treatment.

Commentary: [Extraordinary circumstances to be defined further in Commentary.]

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 should set forth in writing specific reasons for doing so, consistent with Principles 3 and 9, within the period of time specified in law for responding to information requests,

Note: Principle 27 states that the time in which a response must be given to an information request should be set forth in law.

(b) The authority should also provide the requester with sufficient information concerning the the official(s) who authorized non-disclosure and the process for doing so, unless to do so would itself disclose restricted information, and of avenues for appeal, to allow for an examination of the authority's adherence to the law.

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, collected, or produced, the authority should make reasonable efforts to gather the missing information for potential disclosure to the requester.[18]

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

(b) When a document is untraceable or information is said to be non-existent, the public authority under oath should indicate all of the procedures undertaken to try to recover or reconstruct it in such a way that such procedures may be subject to judicial review.

Note: When a document or information that is required by law to be maintained is untraceable, the matter should be referred to police or administrative authorities for investigation. The outcome of the investigation should be made public.

Commentary: [Define what constitutes under oath.]

(c) The duty to search for information is particularly high when the information concerns alleged gross human rights violations.[19]

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 sever and disclose the non-exempt information.

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.

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 independent body if available, and judicial review should be established by law and should be as short as practicably possible.

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 be given. See www.right2info.org/laws. Where time limits for responding to requests are not set forth in law, the time limit should be no more than 30 days. Laws may provide for different time limits in order to take account of different volumes and levels of complexity and sensitivity of documents.

(b) Expedited time limits should apply where there is a demonstrated need for the information on an urgent basis, such as where the information is necessary to safeguard the life or liberty of a person.

[19] See Inter-American Court of Human Rights, *Gomes Lund (Guerrillas of Araguaia) v. Brazil*, paras __.

Principle 28: Right to Review of Decision Withholding Information

(a) A requester has the right to a speedy and low cost review by an independent authority of a refusal to disclose information, or of matters related to the request.

Commentary: A refusal may include an implicit or silent refusal. Matters related to the request subject to a review by an independent authority include fees, timelines and format.

(b) The independent authority should have the competence and resources necessary to ensure an effective review, including full access to all relevant information, even if classified.

(c) A person may challenge a decision of the independent authority before a court in such as way as to ensure that the person may obtain independent and effective review of all relevant issues by a competent tribunal.

(d) Where a court makes a ruling that withholding information is warranted, it should make publicly available fact-specific reasons and its legal analysis in writing, except in extraordinary circumstances, consistent with Principle 3.

PART IV: JUDICIAL ASPECTS OF NATIONAL SECURITY AND RIGHT TO INFORMATION

Principle 29: General Judicial Oversight Principle

(a) Invocations of national security may not be relied upon to undermine the fundamental right to a fair trial by a competent, independent and impartial tribunal established by law.

(b) Where a public authority seeks to withhold information on the ground of national security in any legal proceeding, a court should have the power to examine the information in determining whether the information may be withheld. A judge should not ordinarily dismiss a challenge without examining the information.

Note: It is good practice that the court should not rely on summaries or affidavits asserting the need for secrecy.

OUTSTANDING ISSUE: Courts should have the power to examine – *or courts* should ordinarily examine…

Commentary: 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) The court should ensure that the person seeking access can, to the maximum extent possible, know and challenge the case advanced by the government for withholding the information.

(d) A court should adjudicate the legality and propriety of a public authority's claim 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.

Commentary: Impropriety includes attempts by government to keep information secret as a way to permit impunity for state actors.

(e) The court should independently assess whether the public authority has properly invoked any basis for non-disclosure; the fact of classification should not be conclusive as to the request for non-disclosure of information. Similarly, the court should assess the nature of any harm claimed by the public authority, its likelihood of occurrence, and the public interest in disclosure, in accordance with the standards defined in Principle 3.

Principle 31: Public Access to Judicial Processes

(a) Invocations of national security may not be relied upon to undermine the fundamental right of the public to access judicial processes.

(b) Court judgments – setting forth all of a court's orders and including the essential findings, evidence and legal reasoning – should be made public, except where the interest of juvenile persons otherwise requires.[20]

(c) The public's right of access to justice should include prompt public access to (i) judicial reasoning; (ii) information about the existence and progress of cases; (iii) written arguments submitted to the court; (iv) court hearings and trials[21]; and (v) evidence in court proceedings that forms the basis of a conviction, unless a derogation of this is justified in accordance with these Principles.

Commentary: 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. [Develop commentary concerning extraordinarily limited circumstances in which evidence might be withheld from the public. See, e.g., Rosenberg case, covert witnesses, informants, etc.]

(d) The public should have an opportunity to contest any claim asserted by the public authority that a restriction on public access to judicial processes is strictly necessary on national security grounds.

---

[20] International law permits no derogation on national security grounds from the obligation to pronounce judgments publicly. See, e.g., ECHR, Art. 6.1 and ICCPR Art. 14.1. The Human Rights Committee has stated that, under Article 14.1 of the ICCPR, "Even in cases in which the public is excluded from the trial, the judgment, including the essential findings, evidence and legal reasoning must be made public, except "where the interest of juvenile persons otherwise requires or the proceedings concern matrimonial disputes or the guardianship of children." "Matrimonial disputes or the guardianship of children" are not included in the Principle given that their relationship to national security is attenuated at best.

[21] 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.

Commentary: Limitations on public access to judicial processes may include the partial or complete closure of a hearing, the sealing of records, the non-disclosure of information, the redaction of a judicial opinion, or any other restriction.

(e) Where a court makes a ruling as to whether a restriction on open access to judicial processes is warranted, it should make publicly available fact-specific reasons and its legal analysis in writing, except in extraordinary circumstances, consistent with Principle 3.

Note: This Principle is not intended to modify a state'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 fairness and impartiality of judicial proceedings; (ii) the proper and more honest conduct of the parties; and (iii) the enhanced accuracy of public comment.

Note: Principles 32 and 33 are included in these principles concerning public *access to information in light of the fact that judicial review, and related disclosures in the context of judicial oversight, are often important means for public disclosure of information.*

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 or deprivation of liberty be based on evidence that the accused has not had an opportunity to review and refute.

[Commentary: Deprivation of liberty may include the investigative or pre-trial stages of criminal proceedings, administrative detentions, immigration detention, or other forms of detention.]

(c) In the interests of justice, a public authority should disclose to the defendant and the defendant's counsel the charges against a person and any information necessary to ensure a fair trial, regardless of whether the information is classified, consistent with Principles 3, 10, 30 and 31 [and…], including a consideration of the public interests.

Commentary: 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 should be strictly necessary and in such case, the court should enable the defendant to have substantially the same ability to respond to the charges as the person would have had if the person had access to the information. Commentary will elaborate on fair trial rights as relevant to this principle, including obligation to disclose information the public authority intends to use against a defendant, any potentially exculpatory evidence and any information that may assist the defendant in obtaining a reduction in sentence. 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.

(d) Where the public authority declines to disclose information necessary to ensure a fair trial, the court should stay or dismiss the charges.

Note: The public authorities should not rely on information to their benefit when claiming secrecy, although they may decide to keep the information secret and suffer the consequences.

Commentary: Any stay should be for a limited time to ensure adherence to fair trial rights.

Principle 33: Party Access to Information in Civil Cases

(a) All claims of withholding of information by a public authority should be reviewed in a manner consistent with Principles 3, 10, 30 and 31 [and…], including a consideration of the public interests.

(b) Victims of human rights violations are entitled to an effective remedy and reparation, including public disclosure of abuses suffered. Public authorities should not withhold information material to their claims in a manner inconsistent with this right.

[Commentary: UNGA resolution – remedy and reparation may include public disclosure of abuses suffered to the extent not causing further harm.]

(c) The public also has the right to information concerning gross human rights violations and serious violations of international humanitarian law.

[Commentary: Consider whether and how risk of harm or invasion of privacy of the victim limits the public's right to truth. From UN GA resolution on right to truth and Inter-American and European Court caselaw. See that language in revised Principle 10: The names and other personal data of persons who have been deprived of liberty, who have died in custody, or whose deaths have been caused by the state, may be withheld from disclosure to the general public in order to protect the right to privacy if the person, or in the case of deceased persons, their family members, have expressly and voluntarily so requested, and if the withholding is consistent with human rights. Even in such circumstances, however, this should not preclude publication of aggregate or otherwise anonymous data]

Commentary should analyse public interest analysis in various cases – i.e., when a person makes a credible claim that the authority has violated his or her rights; a public authority making a claim against a person.]

PART V: BODIES THAT OVERSEE THE SECURITY SECTOR

Principle XX: Establishment of Independent Oversight Bodies

States should establish, if they have not already done so, independent oversight bodies to oversee the security sector, including their operations, policies, finances and administration. Such bodies should be institutionally and operationally (including budgetary) independent from the institutions that they are mandated to oversee.

Note: the type and jurisdiction of independent oversight bodies varies from state to state. Examples of such bodies may include: legislative committees, supreme audit institutions, human rights commissioners, ombuds institutions, information and data protection commissioners, and expert intelligence oversight institutions.

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

(a) Independent oversight bodies should have legally guaranteed access to all information necessary for the fulfillment 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.

(b) 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 held by persons whom overseers deem to be relevant for their oversight functions.

(c) Any obligation of public personnel to maintain secrecy or confidentiality should not prevent them from providing information to oversight institutions. The provision of such information should not be considered a breach of any law or contract imposing such obligations.

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

(a) Independent oversight bodies should have adequate legal powers in order to be able to access and interpret any relevant information that they deem necessary to fulfill their mandates.

(i) 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.

(ii) Independent 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 fulfillment of their mandates, with the full cooperation of law enforcement agencies, where required.

(b) Independent 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.

(c) Independent 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.

(d) The law should require security sector institutions to afford independent oversight bodies the cooperation they need to access and interpret the information required for the fulfillment of their functions.

(e) The law should require security sector institutions to make proactive and timely disclosures to independent oversight bodies of specific categories of information that overseers have determined are necessary for the fulfillment 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 Independent Oversight Bodies

A. Applicability of Access to Information Laws

Laws regulating the fulfillment of the public right to access information held by public authorities should apply to security sector oversight bodies.

B. Reporting

(1) Independent oversight bodies should be legally required to produce periodic reports and to make these reports publicly available. These reports should include, at a minimum:

(a) Information on the oversight body itself, including its mandate, membership, budget, performance and activities; and
(b) [Information on the structure, mandate, general activities, and budget of the security sector institutions that fall under their mandate.]

(2) Independent oversight bodies should also provide public versions of their reports relating to thematic and case-specific studies and investigations, and should provide as much information as possible concerning matters of public interest, including those areas listed in Principle 10.

(3) In their [public] reporting, independent oversight bodies should respect privacy rights of all individuals concerned.

(4) Independent oversight institutions should give the institutions subject to their oversight 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

(1) The legal basis for oversight bodies, including their mandates and powers, should be publicly available and easily accessible.

(2) Independent oversight bodies should create mechanisms and facilities for people who are illiterate, speak minority languages, or are visually or aurally impaired to access information about their work.

(3) Independent 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.

(4) Independent oversight bodies should have mechanisms that can effectively preserve the confidentiality of the complaints and the anonymity of the complainant.

Principle 37: Measures to Protect Information Handled by Security Sector Oversight Bodies

(1) The law should require independent oversight bodies to implement all necessary measures to protect information in their possession.

(2) Legislatures should [have the power to] decide whether (i) members of legislative oversight committees, and (ii) heads and members of independent, non-legislative oversight bodies should be subject to security vetting prior to their appointment.

(3)

(4) Where security vetting is required, it should be conducted: (i) in a timely manner, (ii) in accordance with established principles; (iii) free from political bias or motivation; and (iv) whenever possible, by an institution that is not subject to oversight by the body whose members/staff are being vetted.

(5)

(6) Subject to the Principles in Parts VI and VII, members or staffers of independent oversight bodies who disclose classified or otherwise confidential material outside of the body's ordinary 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 any 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 SHOWING WRONGDOING

Principle 39: Categories of Wrongdoing

Disclosures of information, regardless of its classification, which shows wrongdoing which falls into one of the following categories should be considered to be "protected disclosures" if they comply with the conditions set out in Principles 40–42. Disclosures can pertain to wrongdoing that has occurred, is occurring or is likely to occur.

(a) criminal offences;
(b) human rights violations;
(c) international humanitarian law violations;
(d) corruption;
(e) dangers to public health and safety;
(f) dangers to the environment;
(g) abuse of public office;

(h) miscarriages of justice;
(i) mismanagement or waste of resources;
(j) retaliation for disclosure of any of the above listed categories of wrongdoing; and
(k) deliberate concealment of any matter falling into to one of the above categories.

Principle 40: Grounds, Motivation and Proof for Disclosures of Information Showing Wrongdoing

(1) The law should protect from retaliation, as defined in Principle 44, public personnel who make disclosures of information showing wrongdoing, regardless of whether the information is classified or otherwise confidential, so long as, at the time of the disclosure,
   (a) the person making the disclosure had reasonable grounds to believe that the information disclosed (i) was true and (ii) related to one of the categories of wrongdoing set forth in Principle 39; and
   (b) the disclosure complies with the conditions set forth in Principles 41-43.

(2) The motivation for a protected disclosure is irrelevant except where the disclosure is knowingly untrue.

(3) A person making a protected disclosure should not be required to produce supporting evidence or bear the burden of proof in relation to the disclosure.

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

A. Internal Disclosures

The law should require public authorities to establish internal procedures and designate persons to receive protected disclosures.

B. Disclosures to Independent Oversight Bodies

(1) States should also establish or identify independent bodies to receive and investigate protected disclosures. Such bodies should be institutionally and operationally independent from the security sector and other authorities from which disclosures may be made, including the executive branch.

(2) Public personnel should be [authorised] to make protected disclosures to independent oversight bodies or to another body competent to investigate the matter without first having to make the disclosure internally.

(3) The law should guarantee such bodies access to all relevant information and afford them the necessary investigatory powers to ensure this access. Such powers should include subpoena powers and the power to require that testimony is given under oath or affirmation.

C. Obligations of Internal and Independent Oversight Bodies Receiving Disclosures

If a person makes a protected disclosure, as defined in Principle 39, internally or to an independent oversight body, the body receiving the disclosure should be obliged to:

(1) investigate and take prompt measures with a view to resolving the matters in a legally-specified period of time, or refer it to an oversight body that is authorised and competent to investigate, after having consulted the person who made the disclosure;
(2) protect the [confidentiality] [identity] of public personnel who seek to make confidential submissions; anonymous submissions should be considered on their merits;
(3) protect the information disclosed and the fact that a disclosure has been made except to the extent that further disclosure of the information is necessary to remedy the wrongdoing;
(4) notify the person making the disclosure [of the progress and] [of at least the] completion of an investigation and, as far as possible, the steps taken or recommendations made;

Commentary: Any investigation should be free from unnecessary administrative impediments.

Principle 43: Protection of Public Disclosures

The law should protect from retaliation, as defined in Principle 44, disclosures to the public of information concerning wrongdoing as defined in Principle 39, if the disclosure meets the following criteria:

(a) (1) The person made a disclosure of substantially the same information internally and/or to an independent oversight body and:
    (i) the body to which the disclosure was made refused or failed to investigate the disclosure effectively, in accordance with applicable international standards; or
    (ii) the person did not receive a [reasonable] [and appropriate] outcome within a legally-defined period of time.

    Commentary: [will include applicable international standards corresponding to 43(a)(1)(i)].

    OR

    (2) The person reasonably believed that there was a significant risk that making the disclosure internally and/or to an independent oversight body would have resulted in the destruction or concealment of evidence, interference with a witness, or retaliation against the person or a third party;

    OR

    (3) There were no established internal bodies or independent oversight bodies to which a disclosure could have been made;

    OR

    (4) The disclosure relates to an act or omission that constitutes a serious and imminent risk of danger to the life, health and safety of persons, or to the environment.

AND

(b) The person making the disclosure only disclosed the amount of information that was reasonably necessary to bring to light the wrongdoing;

AND

(c) The person making the disclosure reasonably believed that the public interest in having the information revealed outweighed the harm done by its disclosure.

Commentary: Information revealing the identities of covert agents or sources will, in all but the most exceptional cases, not be "reasonably necessary to bring to light the wrongdoing" in question. In cases in which the revelation of such information might be necessary, the interest in maintaining the secrecy of such information, and any dangers to the life, liberty, or security of persons, will presumably be given considerable weight in the assessment of the public interest in disclosure versus the public interest in non-disclosure.

Principle 44: Protection against Retaliation for Making Disclosures of Information Showing Wrongdoing

A. Immunity from Civil and Criminal Liability for Protected Disclosures

A person who has made a disclosure, in accordance with Principles 39-43, shall not be subject to:

(1) Criminal proceedings[, including but not limited to prosecution] for the disclosure of classified or otherwise confidential information; or
(2) Civil proceedings related to the disclosure of classified or otherwise confidential information, including but not limited to attempts to claim damages and defamation proceedings.

B. Prohibition of Other Forms of Retaliation

(1) The law should prohibit retaliation against any person who has made, is suspected to have made, or may make a disclosure in accordance with Principles 39-43.

(2) Prohibited forms of retaliation include, but are not limited to, the following:

(a) Administrative measures or punishments, including but not limited to: letters of reprimand, retaliatory investigations, demotion, transfer, failure to promote, termination of employment, actions likely or intended to damage a person's reputation, or suspension or revocation of a security clearance;
(b) Physical or emotional harm or harassment; or
(c) Threats of any of the above.

(3) Action taken against individuals other than the person making the disclosure may, in certain circumstances, constitute prohibited retaliation.

C. Investigation of Retaliation by an Independent Oversight Body and Judicial Authorities

(1) Any person should have the right to report to an independent oversight body and/or to a judicial authority retaliation, or the threat of retaliation, in relation to protected disclosures.

(2) Independent oversight bodies should be required to investigate a reported retaliation or threat of retaliation. Such bodies should also have the ability to launch investigations in the absence of a report of retaliation.

(3) Independent oversight bodies should be given the powers and resources to investigate effectively any claimed retaliation, including the powers to subpoena persons and records and hear testimony under oath or affirmation.

(4) Independent oversight bodies should make every effort to ensure that proceedings concerning asserted retaliation are fair and in accordance with due process standards.

(5) Independent oversight bodies should have the authority to require the public authority concerned to take remedial or restorative measures, including, but not limited to reinstatement; reassignment; and/or the payment of legal fees, other reasonable costs, back pay and related benefits, travel expenses, and/or compensatory damages.

(6) Independent oversight bodies may also enjoin a public authority from taking retaliatory measures.

(7) Such bodies should complete their investigation into reported retaliation within a legally-defined period of time.

(8) Such bodies should notify relevant persons [of the progress and] [of at least the] completion of an investigation and, as far as possible, the steps taken or recommendations made;

(9) Persons may also appeal a determination that actions in response to the disclosure do not constitute retaliation, or the remedial or restorative measures, of the independent oversight body to a judicial authority.

D. Burden of Proof

If a public authority takes any action adverse to any person, the authority bears the burden of demonstrating that the action was unrelated to the disclosure.

E. No waiver of rights and remedies

The rights and remedies provided for under Principles 39–44 may not be waived or limited by any agreement, policy, form or condition of employment, including by any pre-dispute arbitration agreement. Any attempt to waive or limit these rights and remedies should be considered void.

Principle 45: Encouraging and Facilitating Protected Disclosures

States should encourage public officials to make protected disclosures. In order to facilitate such disclosures, states should require all public authorities to issue guidelines that give effect to Principles 39-44.

Note: Such guidelines should provide, at a minimum: (1) advice regarding the rights and/or responsibilities to disclose wrongdoing; (2) the types of information that should or may be disclosed; (3) required procedures for making such disclosures; and (4) protections provided for by law.

Principle 46: Public Interest Defence for Public Personnel

(a) The law should provide a public interest defence for public personnel subject to criminal or civil proceedings relating to their having made a disclosure of information showing wrongdoing where:

(i) The information does not fall into one of the categories outlined in Principle 39; or
(ii) The disclosure contains information that falls into one of the categories outlined in Principle 39 but is not made in accordance with the procedures outlined in Principles 40–45.

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

(i) whether the person had reasonable grounds to believe that the disclosure would be in the public interest;
(ii) whether the extent of the disclosure was reasonably necessary to disclose the wrongdoing;
(iii) 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 41–43;
(iv) the extent and risk of harm created by the disclosure; and
(v) the existence of exigent circumstances justifying the disclosure.

Note: This Principle is not intended to limit any freedom of expression rights already available to public personnel or any of the protections granted under Principles 39-43.

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

Principle 47: 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 sanctioned for releasing information that they reasonably and in good faith believed could be disclosed pursuant to law.

Principle 47*bis* : Limitations on Criminal Penalties for the Disclosure of Information by Public Personnel

Public disclosure of information, by public personnel, that is not protected by Part VI, should not be subject to criminal penalties. Exceptionally, if the law imposes criminal penalties for

the unauthorised disclosure of information to the public or to persons with the intent that the information will be made public the following conditions should apply:

(a) Criminal penalties should apply only to the disclosure of narrow categories of information that are clearly set forth in law.
(b) The disclosure should pose a real and identifiable risk of causing significant harm.
(c) Any criminal penalty should be set forth in law and as applied should be proportional to the harm caused.
(d) The person should be able to raise the public interest defence, as outlined in Principle 46.

Note: The categories of information that could be subject to criminal penalties consistent with this Principle include the following, and should be similar in terms of specificity and impact on national security: technological data about nuclear weapons; intelligence sources, codes and methods; diplomatic codes; identities of covert agents; and inventions in which the government has an ownership interest and knowledge of which could harm national security.

Principle 48: 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 independent 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: Good practice is to disclose information within a certain defined period of time. 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 49: Protection Against Sanctions for the Possession and Dissemination of Classified Information by Persons Without Authorized Access.

(a) A person who does not have authorised access to classified information may not be sanctioned for the receipt, possession, or disclosure to the public of classified information.

(b) A person who does not have authorised access to classified information may not be subject to charges for conspiracy or other crimes based on the fact of having sought and obtained the information.

Note: This principle is not intended to preclude the prosecution of a person for other crimes committed in the course of seeking or obtaining the information[, such as blackmail, assault, or torture]. This explicitly does not include the possibility of criminal prosecution for the acquisition or reproduction of the information.

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

Commentary; The Joint Declaration of Special Rapporteurs on Wikileaks (2010) stated: "Public 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. In addition, government 'whistleblowers' releasing information on violations of the law, on wrongdoing by public bodies, on a serious threat to health, safety or the environment, or on a breach of human rights or humanitarian law should be protected against legal, administrative or employment-related sanctions if they act in good faith. Any attempt to impose subsequent liability on those who disseminate classified information should be grounded in previously established laws enforced by impartial and independent legal systems with full respect for due process guarantees, including the right to appeal".

Principle 50: Protection of Sources

No 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.

Note: This Principle refers only to investigations concerning unauthorized disclosure of information, not to other crimes.

Principle 51: Prior Restraint

(a) Prior restraints against publication in the interest of protecting national security should be prohibited.

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

Commentary: Article 13.2 of the American Convention provides that "The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability".

(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.

Note: This Principle is not intended 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.[22] *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 52: 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, or any provisions of national or international law that would provide greater protection for disclosures of information by public personnel or others.

[22] The Observer and Guardian v. UK and The Sunday Times v. UK (No. 2), Judgments of 26 November c1991, 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).