GLOBAL PRINCIPLES ON NATIONAL SECURITY AND THE RIGHT TO INFORMATION

("THE TSHWANE PRINCIPLES")

finalized in Tshwane, South Africa
issued on 12 June 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, good practices, and the writings of experts.

They 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 were drafted by 22 organizations and academic centres (listed in the Annex) in consultation with more than 500 experts from more than 70 countries at 14 meetings held around the world, facilitated by the Open Society Justice Initiative, and in consultation with the four special rapporteurs on freedom of expression and/or media freedom and the special rapporteur on counter-terrorism and human rights:

- the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression,
- the UN Special Rapporteur on Counter-Terrorism and Human Rights,
- the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information,
- the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, and
- the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media.

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 enjoy the right of access to information—at least in law, if not in practice. People in these countries are—often for the first time—grappling with the question of whether and under what circumstances information may be kept secret. Other developments contributing to an increase in proposed secrecy legislation have been government responses to terrorism or the threat of terrorism, and an interest in having secrecy regulated by law in the context of democratic transitions.

GLOBAL PRINCIPLES ON NATIONAL SECURITY AND THE RIGHT TO INFORMATION

("THE TSHWANE PRINCIPLES")

finalized in Tshwane, South Africa
issued on 12 June 2013

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 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, the Declaration of Principles on Freedom of Expression in Africa, and the Model Law on Access to Information for Africa;

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; 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;

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, 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 there are international principles—such as those included in the Model Law on Access to Information in Africa, the UN Guiding Principles on Business and Human Rights ("Ruggie Principles"), the Arms Trade Treaty, the OECD Guidelines for Multinational Enterprises, and the Montreux Document on pertinent international legal obligations and good practices for states related to operations of private military and security companies during armed conflict—that recognize the critical importance of access to information from, or in relation to, business enterprises in certain circumstances; and that some expressly address the need for private military and security companies operating within the national security sector to make certain information public;

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;

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 conduct 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 certain information that should not be withheld on national security grounds may potentially 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 public 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 concerning some of the most challenging issues at 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:

"**Business enterprise within the national security sector**" means a juristic person that carries on or has carried on any trade or business in the national security sector, but only in such capacity; either as a contractor or supplier of services, facilities, personnel, or products including, but not limited to, armaments, equipment, and intelligence. This includes private military and security companies (PMSCs). It does not include juristic persons organized as non-profits or as non-governmental organizations.

"**Independent**" means institutionally, financially, and operationally free from the influence, guidance, or control of the executive, including all security sector authorities.

"**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, facts, opinion, advice, memoranda, data, statistics, books, drawings, plans, maps, diagrams, photographs, audio or visual records, documents, emails, logbooks, samples, models, and data held in any electronic form.

"**Information of public interest**" refers to information that is of concern or benefit to the public, not merely of individual interest and whose disclosure is "in the interest of the public," for instance, because it is useful for public understanding of government activities.

"**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 real 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.

"**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.

"**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.

"**Public personnel**" or "**public servant**" refers to current and former public employees, contractors, and sub-contractors of public authorities, including in the security sector. "Public personnel" or "public servant" also include persons employed by non-state bodies that are owned or controlled by the government or that serve as agents of the government; and 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**," when used as a noun, refers to any form of penalty or detriment, including criminal, civil and administrative measures. When used as a verb, "sanction" means to bring into effect such form of penalty or detriment.

"**Security sector**" is defined to encompass: (i) security providers, including but not limited to the armed forces, police and other law enforcement bodies, paramilitary forces, and intelligence and security services (both military and civilian); and (ii) all executive bodies,

departments, and ministries responsible for the coordination, control, and oversight of security providers.

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) International principles also recognize that business enterprises within the national security sector, including private military and security companies, have the responsibility to disclose information in respect of situations, activities, or conduct that may reasonably be expected to have an impact on the enjoyment of human rights.

(c) Those with an obligation to disclose information, consistent with Principles 1(a) and 1(b), must make information available on request, subject only to limited exceptions prescribed by law and necessary to prevent specific, identifiable harm to legitimate interests, including national security.

(d) Only public authorities whose specific responsibilities include protecting national security may assert national security as a ground for withholding information.

(e) Any assertion by a business enterprise of national security to justify withholding information must be explicitly authorized or confirmed by a public authority tasked with protecting national security.

Note: The government, and only the government, bears ultimate responsibility for national security, and thus only the government may assert that information must not be released if it would harm national security.

(f) Public authorities also have an affirmative obligation to publish proactively 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 as identified in Principle 1 where the government asserts or confirms 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, when public authorities assert other public grounds for restricting access—including international relations, public order, public health and safety, law enforcement, future provision of free and open advice, effective policy formulation, and economic interests of the state—they 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, where used to limit the right to information, to be defined precisely in a country's legal framework in a manner consistent with a democratic society.

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.

(b) *Necessary in a democratic society*.

(i) Disclosure of the information must pose a real and identifiable risk of significant harm to a legitimate national security interest.
(ii) The risk of harm from disclosure must outweigh the overall public interest in disclosure.
(iii) The restriction must comply with the principle of proportionality and must be the least restrictive means available to protect against the harm.
(iv) The restriction must not impair the very essence of the right to information.

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

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

"Public interest" is not defined in these Principles. A list of categories of especially high public interest that should be published proactively and should never be withheld is set forth 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 37.

In balancing the risk of harm against the public interest in disclosure, account should be taken of the possibility of mitigating any harm from disclosure, including through means that require 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 risk of harm:

- *factors favoring 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 favoring 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 a country's economy would be relevant in determining whether information should be withheld on that ground, but not on national security grounds.

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: Any person who seeks access to information should have a fair opportunity to challenge the asserted basis for a risk assessment before an administrative as well as a judicial authority, consistent with Principles 26 and 27.

(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.

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, and any component offices of the foregoing—may be exempted from disclosure requirements.

(b) Information may not be withheld on national security grounds simply on the basis that it was generated by, or shared with, a foreign state or inter-governmental body, or a particular public authority or unit within an authority.

Note: Concerning information generated by a foreign state or inter-governmental body, see Principle 9(a)(v).

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 32. 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 35.

Principle 7: Resources

States should devote adequate resources and take other necessary steps, such as the issuance of regulations and proper management 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 consistent with the state's other obligations under international law, and does not involve discrimination of any kind.

Note: Certain aspects of the right to seek, receive, and impart information and ideas are so fundamental to the enjoyment of non-derogable rights that they should always be fully respected even in times of public emergency. As a non-exhaustive example, some or all of the information in Principle 10 would be of this character.

PART II: INFORMATION THAT 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, the information is held by a public authority, and the information falls within one of the following categories:

(i) Information about on-going defence plans, operations, and capabilities for the length of time that the information is of operational utility.

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, or plans.

(ii) Information about the production, capabilities, or use of weapons systems and other military systems, including communications systems.

Note: Such information includes technological data and inventions, and information about production, capabilities, or use. Information about budget lines concerning weapons and other military systems should be made available to the public. See Principles 10C(3) & 10F. It is good practice for states to maintain and publish a control list of weapons, as encouraged by the Arms Trade Treaty as to conventional weapons. It is also good practice to publish information about weapons, equipment, and troop numbers.

(iii) Information about specific measures to safeguard the territory of the state, critical infrastructure, or critical national institutions (*institutions essentielles*) against threats or use of force or sabotage, the effectiveness of which depend upon secrecy;

Note: "Critical infrastructure" refers to strategic resources, assets, and systems, whether physical or virtual, so vital to the state that destruction or incapacity of such resources, assets, or systems would have a debilitating impact on national security.

(iv) Information pertaining to, or derived from, the operations, sources, and methods of intelligence services, insofar as they concern national security matters; and

(v) Information concerning national security matters that was supplied by a foreign state or inter-governmental body with an express expectation of confidentiality; and other diplomatic communications insofar as they concern national security matters.

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

Note: To the extent that particular information concerning terrorism, and counter-terrorism measures, is covered by one of the above categories, the public's right of access to such information may be subject to restrictions on national security grounds in accordance with this and other provisions of the Principles. At the same time, some information concerning terrorism or counterterrorism measures may be of particularly high public interest: see e.g., Principles 10A, 10B, and 10H(1).

(b) It is good practice for national law to set forth an exclusive list of categories of information that are at least as narrowly drawn as the above categories.

(c) A state may add a category of information to the above list of categories, but only if the category is specifically identified and narrowly defined and preservation of the information's secrecy is necessary to protect a legitimate national security interest that is set forth in law, 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 Favor 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 favor 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 systematic or widespread violations of the rights to personal liberty and security. Such information may not be withheld on national security grounds in any circumstances.

(2) Information regarding other violations of human rights or humanitarian law is 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 transitional justice during which the state is especially required to ensure truth, justice, reparation, and guarantees of non-recurrence, there is an overriding public interest in disclosure to society as a whole of information regarding human rights violations committed under the past regime. A successor government should immediately protect and preserve the integrity of, and release without delay, any records that contain such information that were concealed by a prior government.

Note: See Principle 21(c) regarding the duty to search for or reconstruct information about human rights violations.

(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 or are occurring, and applies regardless of whether the violations were committed by the state that holds the information or others.

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

(a) A full description of, and any records showing, 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, so long as consistent with the privacy and other rights of the victims, their relatives, and witnesses; and aggregate and otherwise anonymous data concerning their number and characteristics that could be relevant in safeguarding human rights.

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 persons concerned or, in the case of deceased persons, their family members, expressly and voluntarily request withholding, or withholding is otherwise manifestly consistent with the person's own wishes or the particular needs of vulnerable groups. Concerning victims of sexual violence, their express consent to disclosure of their names and other personal data should be required. Child victims (under age 18) should not be identified to the general public. This Principle should be interpreted, however, bearing in mind the reality that various governments have, at various times, shielded human rights violations from public view by invoking the right to privacy, including of the very individuals whose rights are being or have been grossly violated, without regard to the true wishes of the affected individuals. These caveats, however, 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, and information concerning the extent of their command and control.

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

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

Information covered by this Principle includes:

(1) Laws and regulations that authorize the deprivation of life of a person by the state, and laws and regulations concerning deprivation of liberty, including those that address the grounds, procedures, transfers, treatment, or conditions of detention of affected persons, including interrogation methods. There is an overriding public interest in disclosure of such laws and regulations.

Notes: "Laws and regulations," as used throughout Principle 10, include all primary or delegated legislation, statutes, regulations, and ordinances, as well as decrees or executive orders issued by a president, prime minister, minister or other public authority, and judicial orders, that have the force of law. "Laws and regulations" also include any rules or interpretations of law that are regarded as authoritative by executive officials.

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

(2) 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.

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

Note: 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 state agents, may be withheld from disclosure to the general public to the extent necessary to protect the right to privacy if the persons concerned, or their family members in the case of deceased persons, expressly and voluntarily request withholding, and if the withholding is otherwise consistent with human rights. The identities of children who are being deprived of liberty should not be made available to the general public. These caveats, however, should not preclude publication of aggregate or otherwise anonymous data.

C. Structures and Powers of Government

Information covered by this Principle includes, without limitation, the following:

(1) The existence of all military, police, security, and intelligence authorities, and sub-units.

(2) The laws and regulations applicable to those authorities and their oversight bodies and internal accountability mechanisms, and the names of the officials who head such authorities.

(3) 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.

(4) The existence and terms of concluded bilateral and multilateral agreements, and other major international commitments by the state on national security matters.

D. Decisions to Use Military Force or Acquire Weapons of Mass Destruction

(1) Information covered by this Principle includes information relevant to a decision to commit combat troops or take other 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 recognizes 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 revealing all of the details of the operational aspects of the military action in question (see Principle 9).

(2) The possession or acquisition of nuclear weapons, or other weapons of mass destruction, by a state, albeit not necessarily details about their manufacture or operational capabilities, is a matter of overriding public interest and should not be kept secret.

Note: This sub-principle should not be read to endorse, in any way, the acquisition of such weapons.

E. Surveillance

(1) The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.

Note: This information includes: (a) the laws governing all forms of surveillance, both covert and overt, including indirect surveillance such as profiling and data-mining, and the types of surveillance measures that may be used; (b) the permissible objectives of surveillance; (c) the threshold of suspicion required to initiate or continue surveillance; (d) limitations on the duration of surveillance measures; (e) procedures for authorizing and reviewing the use of such measures; (f) the types of personal data that may be collected and/or processed for national security purposes; and (g) the criteria that apply to the use, retention, deletion, and transfer of these data.

(2) The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance.

Notes: This information includes the identity of each government entity granted specific authorization to conduct particular surveillance each year; the number of surveillance authorizations granted each year to each such entity; the best information available concerning the number of individuals and the number of communications subject to surveillance each year; and whether any surveillance was conducted without specific authorization and if so, by which government entity.

The right of the public to be informed does not necessarily extend to the fact, or operational details, of surveillance conducted pursuant to law and consistent with human rights obligations. Such information may be withheld from the public and those subject to surveillance at least until the period of surveillance has been concluded.

(3) In addition, the public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance.

(4) These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance.

Note: It is good practice for public authorities to be required to notify persons who have been subjected to covert surveillance (providing, at a minimum, information on the type of measure that was used, the dates, and the body responsible for authorizing the surveillance measure) insofar as this can be done without jeopardizing ongoing operations or sources and methods.

(5) The high presumptions in favor of disclosure recognized by this Principle do not apply in respect of information that relates solely to surveillance of the activities of foreign governments.

Note: Information obtained through covert surveillance, including of the activities of foreign governments, should be subject to disclosure in the circumstances identified in Principle 10A.

F. Financial Information

Information covered by this Principle includes information sufficient to enable the public to understand security sector finances, as well as the rules that govern security sector finances. Such information should include but is not limited to:

(1) Departmental and agency budgets with headline items;
(2) End-of-year financial statements with headline items;
(3) Financial management rules and control mechanisms;
(4) Procurement rules; and
(5) Reports made by supreme audit institutions and other bodies responsible for reviewing financial aspects of the security sector, including summaries of any sections of such reports that are classified.

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

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.

H. Public Health, Public Safety, or the Environment

Information covered by this Principle includes:

(1) In the event of any imminent or actual threat to public health, public safety, or the environment, all information that could enable the public to understand or take measures to prevent or mitigate harm arising from that threat, whether the threat is due to natural causes or human activities, including by actions of the state or by actions of private companies.

(2) Other information, updated regularly, on natural resource exploitation, pollution and emission inventories, environmental impacts of proposed or existing large public works or resource extractions, and risk assessment and management plans for especially hazardous facilities.

PART III.A: 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: 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 12: 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 13: 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.

Principle 14: Facilitating Internal Challenges to Classification

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

Note: Security sector personnel are flagged as deserving of special encouragement to challenge classification given the heightened cultures of secrecy in security agencies, the fact that most countries have not 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 15: Duty to Preserve, Manage, and Maintain National Security Information

(a) Public authorities have a duty to preserve, manage, and maintain information according to international standards.[1] Information may be exempted from preservation, management, and maintenance 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 is not disclosed.

(c) Each public body should create and make public, and 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 19.

Note: It is good practice to update such lists annually.

[1] These include: International Council on Archives (ICA), *Principles of Access to Archives* (2012); ICA, *Universal Declaration on Archives* (2010; endorsed by UNESCO); Council of Europe, *Recommendation No R(2000)13 on a European policy on access to archives* (2000); Antonio González Quintana, ICA, *Archival policies in the protection of human rights: 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* (2009).

Principle 16: 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.

Note: It is good practice for review to be required by statute at least every five years. Several countries require review after shorter periods.

(b) The classifier should specify the date, conditions, or event on which the classification shall lapse.

Note: It is good practice that this time limit, or specification of conditions or event on which classification lapses, is subjected to periodic review.

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

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

Principle 17: 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 establish 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 declassified by courts, tribunals or other oversight, ombuds, or appeal bodies, should be proactively disclosed or otherwise made publicly accessible (for instance, through harmonization with legislation on national archives or access to information or both).

Note: This Principle is without prejudice to the proviso regarding other grounds for withholding set forth in preambular paragraph 15.

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 III.B: RULES REGARDING HANDLING OF REQUESTS FOR INFORMATION

Principle 18: 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 19: 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, in extraordinary circumstances, the very existence or non-existence of particular 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.

Principle 20: 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: See Principle 25 for the requirement that the time in which a response must be given should be set forth in law.

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

Principle 21: Duty to Recover or Reconstruct 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 recover or reconstruct the missing information for potential disclosure to the requester.

Note: This Principle applies to information that cannot be located for any reason, for instance because it was never collected, was destroyed, or is untraceable.

(b) A representative of the public authority should be required to indicate under oath and within a reasonable and statutorily specified time all of the procedures undertaken to try to recover or reconstruct the information in such a way that such procedures may be subject to judicial review.

Note: When information that is required by law to be maintained cannot be found, the matter should be referred to police or administrative authorities for investigation. The outcome of the investigation should be made public.

(c) The duty to recover or reconstruct information is particularly strong (i) when the information concerns alleged gross or systematic human rights violations, and/or (ii) during a transition to a democratic form of government from a government characterized by widespread human rights violations.

Principle 22: 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 23: 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 24: Duty to Provide Information in Available Formats

Public authorities should provide information in the format preferred by the requester to the extent possible.

Note: This includes, for example, the obligation of public authorities to take appropriate measures to provide information to persons with disabilities in accessible formats and technologies in a timely manner and without additional cost, in accordance with the UN Convention on People with Disabilities.

Principle 25: 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 best practice, in keeping with the requirements set forth in most access to information laws, to prescribe twenty working days or less as the time period in which a

substantive response must be given. Where time limits for responding to requests are not set forth in law, the time limit should be no more than 30 days for a standard request. 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.

Principle 26: 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.

Note: A refusal may include an implicit or silent refusal. Matters 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 should be entitled to obtain independent and effective review of all relevant issues by a competent court or 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, and consistent with Principle 3.

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

Principle 27: 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 court should not ordinarily dismiss a challenge without examining the information.

Note: In keeping with Principle 4(d), the court should not rely on summaries or affidavits that merely assert a need for secrecy without providing an evidentiary basis for the assertion.

(c) The court should ensure that a 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.

(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 28: Public Access to Judicial Processes

(a) Invocation 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 children under eighteen otherwise requires.

Notes: International law permits no derogation on national security grounds from the obligation to pronounce judgments publicly.

Records of juvenile court proceedings should not be made public. Records of other judicial proceedings involving children should ordinarily redact the names and other identifying information of children under the age of eighteen.

(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, 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.

Note: International law concerning fair trial requirements allows courts to exclude all or part of the public from a hearing for reasons of national security in a democratic society, as well as morals, public order, 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 proportionate.

(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.

(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.

Notes: 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.

Principle 29: 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.

(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 3-6, 10, 27 and 28, including a consideration of the public interests.

(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.

Note: Principles 29 and 30 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 30: Party Access to Information in Civil Cases

(a) All claims of withholding of information by a public authority in a civil case should be reviewed in a manner consistent with Principles 3-6, 10, 27 and 28, including a consideration of the public interests.

(b) Victims of human rights violations have a right 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.

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

PART V: BODIES THAT OVERSEE THE SECURITY SECTOR

Principle 31: Establishment of Independent Oversight Bodies

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

Principle 32: 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 33: 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 and employees and contractors of public authorities, request and inspect relevant records, and inspect physical locations and facilities.

(ii) Independent oversight bodies should 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 analyze 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 34: 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, information on the oversight body itself, including its mandate, membership, budget, performance, and activities.

Note: These reports should also include information about the mandate, structure, budget, and general activities of any security sector institution that does not, itself, make such information publicly available.

(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 in respect of those areas listed in Principle 10.

(3) In their public reporting, independent oversight bodies should respect the rights of all individuals concerned, including their right to privacy.

(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 persons in geographically remote locations, may be

facilitated in making 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 35: Measures to Protect Information Handled by Security Sector Oversight Bodies

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

(b) 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.

(c) 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.

(d) Subject to the Principles in Parts VI and VII, members or staff 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 36: Authority of the Legislature to Make Information Public

The legislature should have the power to disclose any information to the public, including information which the executive branch claims the right to withhold on national security grounds, if it deems it appropriate to do so according to procedures that it should establish.

PART VI: PUBLIC INTEREST DISCLOSURES BY PUBLIC PERSONNEL

Principle 37: Categories of Wrongdoing

Disclosure by public personnel of information, regardless of its classification, which shows wrongdoing that falls into one of the following categories should be considered to be a "protected disclosure" if it complies with the conditions set forth in Principles 38-40. A protected disclosure may pertain to wrongdoing that has occurred, is occurring, or is likely to occur.

(a) criminal offenses;
(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 one of the above categories.

Principle 38: Grounds, Motivation, and Proof for Disclosures of Information Showing Wrongdoing

(a) The law should protect from retaliation, as defined in Principle 41, 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:

(i) the person making the disclosure had reasonable grounds to believe that the information disclosed tends to show wrongdoing that falls within one of the categories set out in Principle 37; and
(ii) the disclosure complies with the conditions set forth in Principles 38-40.

(b) The motivation for a protected disclosure is irrelevant except where the disclosure is proven to be knowingly untrue.

(c) 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 39: 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 authorized 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 that independent oversight bodies have 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 Bodies and Independent Oversight Bodies Receiving Disclosures

If a person makes a protected disclosure, as defined in Principle 37, internally or to an independent oversight body, the body receiving the disclosure should be obliged to:

(1) investigate the alleged wrongdoing and take prompt measures with a view to resolving the matters in a legally-specified period of time, or, after having consulted the person who made the disclosure, to refer it to a body that is authorized and competent to investigate;
(2) protect the 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; and
(4) notify the person making the disclosure of the progress and completion of an investigation and, as far as possible, the steps taken or recommendations made.

Principle 40: Protection of Public Disclosures

The law should protect from retaliation, as defined in Principle 41, disclosures to the public of information concerning wrongdoing as defined in Principle 37, if the disclosure meets the following criteria:

(a) (1) The person made a disclosure of the same or substantially similar 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 reasonable and legally-defined period of time.

  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 was no established internal body or independent oversight body to which a disclosure could have been made;

  OR

(4) The disclosure related to an act or omission that constituted 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;

Note: If, in the process of disclosing information showing wrongdoing, a person also discloses documents that are not relevant to showing wrongdoing, the person should nonetheless be

protected from retaliation unless the harm from disclosure outweighs any public interest in disclosure.

AND

(c) The person making the disclosure reasonably believed that the public interest in having the information revealed outweighed any harm to the public interest that would result from disclosure.

Note: The "reasonably believed" test is a mixed objective-subjective test. The person must actually have held the belief (subjectively), and it must have been reasonable for him or her to have done so (objectively). If contested, the person may need to defend the reasonableness of his or her belief and it is ultimately for an independent court or tribunal to determine whether this test has been satisfied so as to qualify the disclosure for protection.

Principle 41: 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 37-40, should 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 37-40.

(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, reassignment of duties, 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 any measure of 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 should also have the authority to enjoin a public authority from taking retaliatory measures.

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

(8) Such bodies should notify relevant persons 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 37–40 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 42: 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 37-42.

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 43: Public Interest Defence for Public Personnel

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

Note: This Principle applies to all disclosures of information that are not already protected, either because the information does not fall into one of the categories outlined in Principle 37 or the disclosure contains information that falls into one of the categories outlined in Principle 37 but was not made in accordance with the procedures outlined in Principles 38-40.

(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 extent of the disclosure was reasonably necessary to disclose the information of public interest;
(ii) the extent and risk of harm to the public interest caused by the disclosure;
(iii) whether the person had reasonable grounds to believe that the disclosure would be in the public interest;
(iv) whether the person attempted to make a protected disclosure through internal procedures and/or to an independent oversight body, and/or to the public, in compliance with the procedures outlined in Principles 38-40; and
(v) the existence of exigent circumstances justifying the disclosure.

Note: Any law providing criminal penalties for the unauthorized disclosure of information should be consistent with Principle 46(b).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 37-42 or 46.

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

Principle 44: Protection Against Penalties for Good Faith, Reasonable Disclosure by Information Officers

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

Principle 45: 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 sanctions, unless an appeal is filed in accordance with procedures set forth in law.

Principle 46: Limitations on Criminal Penalties for the Disclosure of Information by Public Personnel

(a) The public disclosure by public personnel of information, even if not protected by Part VI, should not be subject to criminal penalties, although it may be subject to administrative sanctions, such as loss of security clearance or even job termination.

(b) If the law nevertheless imposes criminal penalties for the unauthorized disclosure of information to the public or to persons with the intent that the information will be made public the following conditions should apply:

(i) Criminal penalties should apply only to the disclosure of narrow categories of information that are clearly set forth in law;

Note: If national law provides for categories of information the disclosure of which could be subject to criminal penalties they should be similar to the following 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 intellectual property in which the government has an ownership interest and knowledge of which could harm national security.

(ii) The disclosure should pose a real and identifiable risk of causing significant harm;

(iii) Any criminal penalty, as set forth in law and as applied, should be proportional to the harm caused; and

(iv) The person should be able to raise the public interest defence, as outlined in Principle 43.

Principle 47: Protection Against Sanctions for the Possession and Dissemination of Classified Information by Persons Who Are Not Public Personnel

(a) A person who is not a public servant may not be sanctioned for the receipt, possession, or disclosure to the public of classified information.

(b) A person who is not a public servant 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 intends to prevent the criminal prosecution for the acquisition or reproduction of the information. However, this Principle is not intended to preclude the prosecution of a person for other crimes, such as burglary or blackmail, committed in the course of seeking or obtaining the information.

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

Principle 48: Protection of Sources

No person who is not a public servant should 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 49: Prior Restraint

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

Note: Prior restraints are orders by judicial or other state bodies banning the publication of specific material already in the possession of a person who is not a public servant.

(b) 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: "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.

PART VIII: CONCLUDING PRINCIPLE

Principle 50: 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.

Annex: Partner Organizations

The following 22 organizations contributed substantially to the drafting of the Principles, and are committed to working to disseminate, publicize, and help implement them.[2] After the name of each organization is the city, if any, in which it is headquartered and the country or region in which it works. Organizations that undertake substantial work in three or more regions are listed as "global."

- Africa Freedom of Information Centre (Kampala/Africa);
- African Policing Civilian Oversight Forum (APCOF) (Cape Town/Africa)
- Alianza Regional por la Libre Expresión e Información (Americas)
- Amnesty International (London/global);
- Article 19, the Global Campaign for Free Expression (London/global);
- Asian Forum for Human Rights and Development (Forum Asia) (Bangkok/Asia);
- Center for National Security Studies (Washington DC/United States);
- Central European University (Budapest/ Europe);
- Centre for Applied Legal Studies (CALS), Wits University (Johannesburg/South Africa);
- Centre for European Constitutionalization and Security (CECS), University of Copenhagen (Copenhagen/Europe);
- Centre for Human Rights, University of Pretoria (Pretoria/Africa);
- Centre for Law and Democracy (Halifax/global);
- Centre for Peace and Development Initiatives (Islamabad/Pakistan);
- Centre for Studies on Freedom of Expression and Access to Information (CELE), Palermo University School of Law (Buenos Aires/Argentina);
- Commonwealth Human Rights Initiative (New Delhi/Commonwealth);
- Egyptian Initiative for Personal Rights (Cairo/Egypt);
- Institute for Defence, Security and Peace Studies (Jakarta/Indonesia);
- Institute for Security Studies (Pretoria/Africa);
- International Commission of Jurists (Geneva/global);
- National Security Archive (Washington DC/global);
- Open Democracy Advice Centre (Cape Town/Southern Africa); and
- Open Society Justice Initiative (New York/global).

.

[2] In addition, Aidan Wills and Benjamin Buckland, of the Geneva Centre for Democratic Control of the Armed Forces (DCAF) but not affiliated with any of the partner organizations, also made especially significant contributions to Part V on Oversight Bodies and Part VI on Public Interest Disclosures, as well as to the Principles as a whole.