GLOBAL PRINCIPLES ON NATIONAL SECURITY AND THE RIGHT TO INFORMATION

"The Tshwane Principles"
finalized in Tshwane, South Africa
issued on 12 June 2013

The Tshwane Principles on National Security and the Right to Information address the question of how to ensure public access to government information without jeopardizing legitimate efforts to protect people from national security threats.

These Principles were drafted by 22 civil society organizations and academic centres, facilitated by the Open Society Justice Initiative, in order to provide guidance to those engaged in drafting, revising, or implementing relevant laws and policies.

Based on international and national law and practices, and more than two years of consultation around the world with government actors, the security sector and civil society, they set out concrete guidelines on the appropriate limits of secrecy, protections for whistleblowers, the parameters of the public's right to information about human rights violations and other issues.

An Overview: Fifteen Things the Principles Say

1. The public has a right of access to government information, including information from private entities that perform public functions or receive public funds. (Principle 1)

2. It is up to the government to prove the necessity of restrictions on the right to information. (Principle 4)

3. Governments may legitimately withhold information in narrowly defined areas, such as defence plans, weapons development, and the operations and sources used by intelligence services. Also, they may withhold confidential information supplied by foreign governments that is linked to national security matters. (Principle 9)

4. But governments should never withhold information concerning violations of international human rights and humanitarian law, including information about the circumstances and perpetrators of torture and crimes against humanity, and the location of secret prisons. This includes information about past abuses under previous regimes, and any information they hold regarding violations committed by their own agents or by others. (Principle 10A)

5. The public has a right to know about systems of surveillance, and the procedures for authorizing them. (Principle 10E)

6. No government entity may be exempt from disclosure requirements—including security sector and intelligence authorities. The public also has a right to know about the existence of all security sector entities, the laws and regulations that govern them, and their budgets. (Principles 5 and 10C)

7. Whistleblowers in the public sector should not face retaliation if the public interest in the information disclosed outweighs the public interest in secrecy. But they should have first made

a reasonable effort to address the issue through official complaint mechanisms, provided that an effective mechanism exists. (Principles 40, 41 and 43)

8. Criminal action against those who leak information should be considered only if the information poses a "real and identifiable risk of causing significant harm" that overrides the public interest in disclosure. (Principles 43 and 46)

9. Journalists and others who do not work for the government should not be prosecuted for receiving, possessing or disclosing classified information to the public, or for conspiracy or other crimes based on their seeking or accessing classified information. (Principle 47)

10. Journalists and others who do not work for the government should not be forced to reveal a confidential source or other unpublished information in a leak investigation. (Principle 48)

11. Public access to judicial processes is essential: "invocation of national security may not be relied upon to undermine the fundamental right of the public to access judicial processes." Media and the public should be permitted to challenge any limitation on public access to judicial processes. (Principle 28)

12. Governments should not be permitted to keep state secrets or other information confidential that prevents victims of human rights violations from seeking or obtaining a remedy for their violation. (Principle 30)

13. There should be independent oversight bodies for the security sector, and the bodies should be able to access all information needed for effective oversight. (Principles 6, 31-33)

14. Information should be classified only as long as necessary, and never indefinitely. Laws should govern the maximum permissible period of classification. (Principle 16)

15. There should be clear procedures for requesting declassification, with priority procedures for the declassification of information of public interest. (Principle 17)

***

Tshwane Principles*: http://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles/.*

Endorsements*: http://www.right2info.org/exceptions-to-access/national-security/global-principles.*

Drafters*: Africa Freedom of Information Centre; African Policing Civilian Oversight Forum; Alianza Regional por la Libre Expresión e Información; Amnesty International; Article 19, the Global Campaign for Free Expression; Asian Forum for Human Rights and Development (Forum Asia); Center for National Security Studies; Central European University; Centre for Applied Legal Studies , University of Witwatersrand; Centre for European Constitutionalization and Security, University of Copenhagen; Centre for Human Rights, University of Pretoria; Centre for Law and Democracy; Centre for Peace and Development Initiatives; Centre for Studies on Freedom of Expression and Access to Information , Palermo University School of Law; Commonwealth Human Rights Initiative; Egyptian Initiative for Personal Rights; Institute for Defence, Security and Peace Studies; Institute for Security Studies; International Commission of Jurists; National Security Archive; Open Democracy Advice Centre; and Open Society Justice Initiative.*