Transparency & ACCOUNTABILITY Initiative

National security transparency and accountability

A guide to best practice in transparency, accountability and civic engagement across the public sector

The Transparency and Accountability Initiative is a donor collaborative that includes the Ford Foundation, Hivos, the International Budget Partnership, the Omidyar Network, the Open Society Foundations, the Revenue Watch Institute, the United Kingdom Department for International Development (DFID) and the William and Flora Hewlett Foundation.

The collaborative aims to expand the impact, scale and coordination of funding and activity in the transparency and accountability field, as well as explore applications of this work in new areas.

The views expressed in the illustrative commitments are attributable to contributing experts and not to the Transparency and Accountability Initiative. The Transparency and Accountability Initiative members do not officially endorse the open government recommendations mentioned in this publication.

For more information contact:

Transparency
& Accountability
Initiative

c/o Open Society Foundation
4th floor, Cambridge House
100 Cambridge Grove
London, W6 0LE UK

Tel: +44 (0)20 7031 0200
E: contact@transparency-initiative.org

www.transparency-initiative.org

National security transparency and accountability

Contributor: Open Society Foundations[1]

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

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

Initial steps

Goal

All public bodies that handle national security information, including the armed forces, ministry of foreign affairs, intelligence and special services, are covered by access to information and proactive disclosure requirements, subject only to specific and limited exceptions approved by the legislature.

Justification

Security sector and other agencies that handle national security information should be covered by access to information laws or other disclosure obligations for at least four reasons:

1. Application of such laws reaffirms both to the entities and the public that security sector agencies, like all public bodies, are subject to the rule of law and democratic accountability.
2. Application of disclosure obligations has led to exposure of wrongdoing, mismanagement and threats to public safety, health and the environment that might not otherwise have come to light.
3. Exceptions in access to information and related laws have proved effective in protecting information that truly does need to remain secret. We are not aware of any instances in which disclosure of information pursuant to an access to information law resulted in harm to national security that exceeded the public interest in knowing the information.
4. Intelligence and security agencies produce a great number of documents that are invaluable to researchers, scholars and the public that do not reveal anything about confidential government actions. For instance, the US Central Intelligence Agency (CIA) holds extensive documents concerning Saddam Hussein's history of human rights abuses. None of these documents reveal anything about US policies or CIA activities, but they do reveal a great deal of information of public interest about what Saddam Hussein did and what and when the US knew about these abuses.

[1] OSF thanks the following organizations for their assistance in developing these sample commitments: Africa Freedom of Information Centre (Africa), American Civil Liberties Union (US), Centre for Applied Legal Studies, Witwatersrand University (South Africa), Centre for National Security Studies (US, international), Centre for Studies on Freedom of Expression and Access to Information (CELE), Palermo University (Argentina, Latin America), Commonwealth Human Rights Initiative (India, Commonwealth), Conectas - Human Rights (Brazil, global south), Egyptian Initiative for Personal Rights (Egypt), Fundar (Mexico), Institute for Information Freedom Development (Russia), Institute for Defense Security and Peace Studies (Indonesia), Institute for Security Studies (Africa), National Security Archive (US, international), Open Democracy Advice Centre (South Africa, southern Africa), OpenTheGovernment.org (US), and Project on Government Oversight (US).

Recommendations

1. States should pass or amend their laws, or the Head of State should issue a decree, to make clear that all public bodies that handle national security information are subject to disclosure requirements. Specific and limited categories of information that must be kept secret to protect the nation's security – such as identities of sources, and intelligence gathering techniques – may be exempted by statute.
2. The existence of all public bodies, including intelligence entities, should be publicly disclosed, as well as contact numbers, budgets and general powers and authorities of such bodies.
3. States should preserve police, military and intelligence archives, should open them to the public to the extent not inconsistent with protecting legitimate national security interests, and should criminalize the willful destruction or alteration of records unless expressly permitted by law.
4. States should establish bodies to review the decisions of security sector agencies to withhold information. Such oversight bodies should be autonomous, adequately resourced, and equipped with the powers needed to fulfill their mandates.
5. No information should remain classified indefinitely. The presumptive maximum period of secrecy on national security grounds should be established by law and should be subject to extension only in exceptional circumstances and by a decision-maker independent of the initial classifier.

Country examples

India's Right to Information Act 2005 applies to all branches of the armed forces, the Ministry of Defense, the Coast Guard, the Department of Atomic Energy, nuclear power plants, aeronautics and space research organizations (except the Aviation Research Centre), and state civilian and armed police organizations.[2] The Act allows intelligence and security services to be exempted from the law,[3] but Parliament can debate any exclusion and force the government to withdraw it. Moreover, all security and intelligence agencies, even those excluded from the purview of the RTI Act, are obliged to disclose information about allegations of corruption and human rights violations committed by their officials and employees.[4] In the US, no agency may be entirely exempted from the Freedom of Information Act (FOIA); only "operational files" of intelligence agencies – e.g., informants' identities, and secret methods of information gathering that would be ineffective if revealed -- may be exempted, and only by a statute duly passed by both Houses of Congress.[5] For instance, a bill to exempt the operational files of the Defense Intelligence Agency was defeated in 2000 because the bill, if passed, would have shielded the activities of foreign death squads, torturers and other human rights abusers.[6] More recently, President Obama ordered that no category of intelligence information may be kept forever secret, and the CIA is now disclosing its highest level President's briefs from the 1960s. The interagency appeals panel (ISCAP) has ruled in favor of disclosing CIA documents in more than 60% of cases, illustrating the value of an appeals panel that is independent, includes representatives of several agencies, and is adequately resourced. Knowing that files may not be kept secret forever has had a significant positive effect on promoting archival programs and good governance in general.

---

[2] Right to Information (RTI) Act, sec. 2(h).

[3] Sec. 24 of India's RTI Act provides that the Central Government and any state governments may add any intelligence or security organization to a list of bodies exempted from the Act.

[4] RTI Act, Sec. 24(2) and (4) require that "information pertaining to allegations of corruption and human rights violations shall not be excluded."

[5] "Operational files" of several intelligence agencies--including the Central Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office and the National Security Agency--are exempted by statute from the FOIA pursuant to 5 U.S.C. § 552 (b)(3), which exempts materials "specifically exempted from disclosure by statute."

[6] See Archive Calls on CIA and Congress to Address Loophole Shielding CIA Records From the FOIA, National Security Archive Electronic Briefing Book No. 138, "Proliferation of the Problem," (Oct. 15, 2004), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB138/index.htm.

More substantial steps

Goal

States make public, and do not classify, information about human rights violations, corruption and other serious wrongdoing, including information needed by victims to obtain redress or by prosecutors to bring criminal charges.

Justification

States increasingly are adopting access to information, secrecy and related laws that expressly state that information about human rights violations, corruption or other serious crimes may not be withheld or classified, and must be provided on request. States have adopted mandatory transparency provisions for several reasons: disclosure of such information deters wrongdoing, facilitates accountability, promotes good governance, and helps victims obtain some satisfaction. Moreover, adherence to the principle of open justice is crucial to guard against excessive judicial deference to the executive and to ensure respect for human rights even during periods when vital national interests are under threat.[7] Only in exceptional circumstances may the high public interest in knowing about torture and other serious abuses be overridden, namely, when the state can establish that disclosure of information would pose an identifiable, likely and significant risk of serious harm to a legitimate and important national security interest.

Recommendations

1. States should pass laws that explicitly state that information about human rights violations, corruption or other serious wrongdoing may not be classified or otherwise withheld from the public. Best practice is to disclose such information proactively.
2. States should commit to not invoke national security as a ground for denying Information that an individual needs either to establish that he/she was the victim of a human rights violation or is not guilty of a criminal offense.

Country examples

The laws of more than a dozen countries – including Albania, Ecuador, Guatemala, India, Mexico, Peru, Romania, Russia and Uruguay – expressly provide that information about human rights violations, violations of law in general, and/or corruption may not, under any circumstances, be classified or withheld, and some provide that such information must be disclosed proactively.[8]

---

[7] See e.g., *R (Binyam Mohamed) v. Secretary of State for Foreign and Commonwealth Affairs* (No 4) [2009] 1 WLR 2653 ["BM (No 4)"], 36; and [Court of Appeal] 131.

[8] Mexico's Federal Transparency and Access to Public Government Information Law 2002 includes a clause in Article 14 that explicitly overrides exceptions when the information is "related to the investigation of a severe violation of fundamental rights or crimes against humanity." Romania's RTI law provides that "information that favors or conceals the violation of the law by a public authority or institution" cannot be classified and should be disclosed in the public interest. Law no. 544/2001 of the 12th of October 2001 on Free Access to Information of Public Interest, Article 13. Article 7 of the Russian Federal Law on State Secrets states that "It is not allowable to classify information regarding violations of human rights and illegal wrongdoing by state bodies and their officials." Albania's Law on Classified Information states that "[c]lassification shall be prohibited when made with the intent of covering up (suppressing) violations of the law, or failures or the ineffectiveness of the state administration; depriving a person, organization or institution of the right of access [to the relevant information]; or preventing or delaying the disclosure of information whose protection is not justified by national security interests." Sec. 10 of Law No. 8457 of Feb 11, 1999 on Prohibition of Classification.

Most ambitious steps

Goal

Mechanisms exist to ensure that public servants, including members of intelligence services and special forces, are able to report evidence of serious wrong-doing to independent oversight bodies without fear of retaliation; public servants are able to report such evidence to the media and public without fear of criminal punishment; and the media and other members of the public are able to publish and disseminate such reports without fear of punishment.

Justification

Numerous regional and national bodies, from the Council of Europe to more than 20 national governments, are currently reviewing their laws and policies to increase protections for public sector personnel who disclose information that reveals serious wrongdoing. It is increasingly recognized that protections for insiders (sometimes called "whistleblowers") is a crucial element of any strategy to effectively combat gross misuse of resources and abuse of power, and to ensure that the public has access to information needed to participate meaningfully in policy making as well as to protect against threats to public safety, health and the environment. Moreover, experience shows that the most effective way to deter leaks of classified or otherwise secret information is through career incentives and disincentives and pursuit of policies that are recognized as legitimate, not through use of criminal law or penalties directed against public servants. Criminal prosecution of media and other information disseminators for reporting government information is inconsistent with democratic principles and freedom of the press. Genuinely sensitive information is best protected through the use of narrowly drawn statutes criminalizing disclosure of clearly defined and limited categories of information whose disclosure would likely cause identifiable and significant harm to national security that is not outweighed by the public interest in knowing such information.

Recommendations

1. Members of the public, including the media, should be able to publish information without fear of criminal prosecution or other official sanction or penalty, in order to safeguard the crucial role of the media and social watchdogs in promoting democratic governance.
2. Public sector personnel, including members of the intelligence services and other security sector agencies, should be authorized, and indeed encouraged, to provide information to oversight bodies of serious wrongdoing, mismanagement, or threats to public safety, health or the environment, without fear of retaliation, so long as they reasonably believe the information to be accurate. Such reports should be properly investigated and appropriate remedial steps taken. Security procedures should be established to enable these disclosures to occur while keeping secret the identity of the whistle-blower as well as, where necessary, the reported information itself.
3. Public sector personnel should not be criminally prosecuted for disclosing to the public information concerning serious wrongdoing, mismanagement, or threats to public safety, health or the environment if they have exhausted internal reporting procedures or if internal reporting would likely be fruitless or subject them to retaliation.
4. Before public sector personnel are subject to sanctions of any sort beyond paid administrative leave for disclosing classified information to the public in violation of any oath, agreement or rule, they first must be afforded full due process rights by law and in practice, including a fair hearing before a body independent of the agency seeking to impose sanctions.
5. No journalist should be compelled to reveal a confidential source or unpublished materials in an investigation concerning unauthorized disclosure of information to the press or public.

Country examples

The European Court of Human Rights ruled in 2008 that the dismissal by the Government of Moldova of an employee in the prosecutor's office for making disclosures to a newspaper concerning pressure from public officials to dismiss criminal proceedings against police officers constituted an unlawful interference with the employee's right to impart information. The unauthorized leak could be justified in light of the lack of an alternative, effective remedy; the public interest in and truthfulness of the information, which outweighed any harm caused by the disclosure; and the employee's good motive.[9] During the period 2007-2010, the Parliamentary Assembly of the Council of Europe undertook a study of whistleblower protection regimes in Europe and other parts of the world and adopted a set of principles to serve as a guide to its member States for instituting similar legislation.[10] These principles include robust protections for "protected disclosures," defined to include "all bona fide warnings against various types of unlawful acts, including all serious human rights violations which affect or threaten the life, health, liberty and any other legitimate interests of individuals as subjects of public administration or taxpayers." Governments throughout Europe, the Americas and other parts of the world have started to domesticate and implement many of these principles.

[9] Guja v. Moldova, Eur. Ct. of Human Rights (2008), App. No. 14277/04.

[10] These principles are contained in Resolution No. 1729 of the Parliamentary Assembly of the Council of Europe, available at: http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta10/ERES1729.htm, last accessed on August 12, 2011.

Transparency
& Accountability
Initiative

c/o Open Society Foundation
4th floor, Cambridge House
100 Cambridge Grove
London, W6 0LE UK

Tel: +44 (0)20 7031 0200
E: contact@transparency-initiative.org

www.transparency-initiative.org