DCAF REGIONAL PROGRAMMES

THE INDONESIAN DRAFT STATE SECRECY LAW

Four International Perspectives

Philipp Fluri (Ed.)

The Geneva Centre for the Democratic Control of Armed Forces

The Indonesian Draft State Secrecy Law

Four International Perspectives

Edited by
Philipp Fluri

Geneva Centre for the Democratic Control
of Armed Forces
(DCAF)
www.dcaf.ch

The Geneva Centre for the Democratic Control of Armed Forces is one of the world's leading institutions in the areas of security sector reform (SSR) and security sector governance (SSG).

DCAF provides in-country advisory support and practical assistance programmes, develops and promotes appropriate democratic norms at the international and national levels, advocates good practices and makes policy recommendations to ensure effective democratic governance of the security sector.

DCAF's partners include governments, parliaments, civil society, international organisations and the range of security sector actors such as police, judiciary, intelligence agencies, border security services and the military.

2010

The Indonesian Draft State Secrecy Law

Four International Perspectives

Edited by
Philipp Fluri

Geneva, 2010

Philipp Fluri, ed., *The Indonesian Draft State Secrecy Law. Four International Perspectives*, DCAF Regional Programmes Series # 3 (Geneva: Geneva Centre for the Democratic Control of Armed Forces, May 2010).

DCAF Regional Programmes Series no. 3

Executive publisher: Procon Ltd., <www.procon.bg>

Cover design: Hristo Bliznashki

ISBN 978-92-9222-141-6

INTRODUCTION

Authoritarian regimes do not only like to foster nationalist thought—thus creating questions to which they are supposedly the answer—they also are characterised by a 'culture' of secrecy which ordinarily surpasses by far the exigencies of defence and is in clear violation of the tenets of accountability and transparency adhered to by democratic, open societies. Denizens of authoritarian systems will grow up being taught that basically everything pertaining to the state and its servants (not the citizens but the bureaucracy in the service of one party, or one family) is necessarily secret. And so the successes and failures of state-owned companies become secret, the fortunes of the ruling class, etc. And a corrupted justice system will see to it that the interests of the so-called elites are kept out of the realm of transparency.

In a democracy not all information is openly available. There are legitimate interests of the democratic government to keep certain well-defined classes of information confidential from foreign powers, but also from their own citizens. The difference is that they do this not in the interest of a ruling class, family, or party, but within defined boundaries with the welfare of the community of citizens, voters and taxpayers in mind. One will find in such societies a stratification of classes of data termed confidential or secret (classification). The question of who may declare data secret, and for whom, and who may un-declare is laid down in law or procedural provisions, along with the circumstances and conditions under which citizens and/or their elected representatives may have access to such information, or sites. There is then a fundamental difference, and the argument by representatives of the authoritarian school of thought that 'democracies have secrecy regulations too' (in justification of their own) just does not hold water.

In what follows we asked leading international experts to look at secrecy legislation and regulations in comparative perspective. As most emerging democracies will go through similar birth pains we hope to give indications as to what is secrecy, who may declare information or objects secret, and under what circumstances.

Philipp Fluri, Ph.D.
Deputy Director DCAF

Geneva, May 2010

CONTENTS

Indonesian Draft Legislation on State Secrets

Ian Leigh

Good Practice

I have been asked to identify good practice in the field of official secrecy legislation. I would identify the following key principles:

(i) Official Secrets legislation should be tightly focused and closely linked to legitimate state security concerns.

(ii) There should be appropriate recognition of the place of disclosure of some kinds of official information in promoting accountability and transparency of public bodies and in fighting corruption, illegality and waste by government officials.

(iii) Legislation should be framed to prevent unnecessary bureaucracy and cost, especially with regard to classification and security clearance.

(iv) Recognition of the special position of the press and its importance in conveying information about government to citizens and voters.

These concerns lead onto the need for strictly limited categories of information to be protected, for robust systems to classify and de-classify information, and for offences that are matched to the damage of disclosure and the public interests in disclosing some official information.

It is instructive to consider the draft legislation with reference to the *Johannesburg Principles on National Security*, *Freedom of Expression and Access to Information* – a set of internationally recognised standards drafted by an expert committee in 1995, set out in full in Appendix 1.[1] The Johannesburg Principles state

[1] These Principles were adopted on 1 October 1995 by a group of experts in international law, national security, and human rights convened by Article 19, the International Centre Against Censorship, in collaboration with the Centre for Applied Legal Studies of the University of the Witwatersrand, in Johannesburg, http://www1.umn.edu/humanrts/instree/johannesburg.html#6. The Johannesburg Principles are endorsed by the UN

that legal restrictions on freedom of expression should be "accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to foresee whether a particular action is unlawful" (Principle 1.1). A government wishing to uphold restriction should bear the burden of establishing that the expression or information at issue poses a *serious* threat, that the *least restrictive means* possible are applied for protecting that interest and that it is compatible with democratic principles (Principle 1.3). Principle 2.b is worth quoting verbatim:

> … a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

In summary it is submitted that in several serious respects the draft legislation does not conform to good practice standards with regard to legislation on official secrets. Comments on the draft legislation are grouped below on the following themes: over-reach of criminal liability; vague and over-broad descriptions of protected information; absence of public interest and other defences; potential liability of journalist and corporations; and excessive penalties. *Specific recommendations appear highlighted in each section.*

Over-Reach of Criminal Liability

The draft legislation fails to distinguish between the very different situations in which official information be disclosed, according to the purpose of the disclosure, i.e. espionage and whistle-blowing are treated identically.

Moreover, it treats anyone involved in the disclosure in the same way, regardless of material differences. The draft legislation fails to distinguish adequately between different groups of people who may be affected by it. Journalists are treated in the same way as civil servants and military personnel and the same as those involved in espionage (foreign agents). These are very different positions in terms of moral culpability and yet the draft offences make no such distinctions since they apply to 'Every Person' (Arts. 42-47).

By contrast, in the UK Official Secrets Act 1989 (set out in Appendix 2) offences apply mainly only to civil servants (Crown servants) and to government contractors. Even within these groups security and intelligence officials are singled out for more stringent controls (s.1 Official Secrets Act 1989). *It is suggested that consid-*

Special Rapporteur on Freedom of Expression, see UN Doc E7CN.4/1996/39, 1996, para. 154.

eration should be given to revising the legislation to rank in seriousness disclosures according to the type of intent and the position of the person concerned.

Vague and/or Over-Broad Descriptions of Protected Information

In several places the scope of the information protected is vague and/or overbroad. This applies both to the meaning of state secrets (Article 6) and to the categories of classified information.

Meaning of State Secrets

The categories of state secrets are described in Article 6. These are information related to: state defence, relating to the Indonesian National Armed forces, related to intelligence, encryption, to foreign relations, and to national economic resilience. Each of these is discussed below.

State Defence (Art. 6(1))

The categories of information covered here are very broad and include a number of items which one would expect to be public knowledge in a democracy and indeed knowledge of which is necessary for effective parliamentary accountability of the military: especially items (h), (j) and (m). It is suggested that references to these items be deleted.

Relating to the Indonesian National Armed Forces (Art. 6(2))

The categories of information are broadly appropriate, since they relate mainly to technical/operational detail. *The difficulty remains, however, of how if at all journalists can legitimately report military operations in times of conflict without breaching the draft Act, since practically all aspects of deployment would appear to be regarded as state secrets.*

Related to intelligence (Art. 6(3))

Most of the categories specified here are clearly appropriate and are related the operational functioning of the intelligence services. *However, in one or two instances there could be a legitimate public or parliamentary interest, having regard to the accountability of the services. These are: (m) referring to 'Information related to organizing techniques. … geared at protecting information classified as state secrets' and (p) 'Data on the function of the protection system of information classified as state secrets.' In both cases thee seem to be procedural matters for which there is no obvious justification for treating as secret. The inclusion of (r) seems inappropriate as it does not obviously refer to intelligence.*

Encryption (Art. 6(4))

The inclusion of these matters is clearly appropriate.

Foreign relations (Art. 6(5))

This refers to the usual categories of protected diplomatic information. Although arguably these are over-broad, Indonesian legislation is not unusual in that respect.

National economic resilience (Art. 6(6))

Headings (e) and (f) seem appropriate. *The generalised protection given to national economic interests under headings (a)–(d) is inappropriately broad and has the potential to interfere with much routine commercial activity, political discussion of economic performance and business journalism. Heading (c) in particular is breath-takingly broad bearing in mind the severe criminal penalties attached to breach. I am doubtful also if it is appropriate at all to treat disclosures in category (a) as a criminal matter.*

In addition to these specific lists of state secrets there also appears a very vaguely-worded sweeping-up provision: (b) (sic) "Type of other state secrets as stipulated in Article 3 exempted by the law and which brings about consequences as mentioned in Article 7, Article 8, and Article 9." This provision is virtually *meaningless* as it stands since the '*Types of state secrets*' "stipulated" in Article 3 are: "a) information; b) object and/or facility, and c) activity." The only qualification, therefore, is by reference to the *consequences* of disclosure under Articles 7, 8 and 9. These provisions define 'highly confidential,' 'confidential' and 'limited confidentiality' state secrets by reference to the degree of harm caused by their disclosure. Consequently provision (b) runs contrary to the structure of the remainder of the Act which criminalizes disclosure of certain types of state secrets according to the damage of disclosure; provision (b) effectively imposes liability according to damage regardless of what the information is about. If this provision is retained, Articles 6(1)–(6) can be by-passed in all instances and the whole scheme of the Act is subverted. *Article 6 Paragraph (b) should be deleted from the draft Act.*

Categories of Classified Information

Commentators have noted that intelligence agencies and governments tend "to overclassify (indiscriminate classification) and to resist efforts to declassify documents after a period of time."[2] It is not merely the case that innocuous information

[2] Marina Caparini, "Challenges of Control and Oversight of Intelligence Services in a Liberal Democracy," paper presented at the workshop "Democratic and Parliamentary Oversight of Intelligence Services," Geneva Centre for the Democratic Control of the

may be prevented from disclosure. The economic costs of maintaining an over-broad system for classifying information and vetting the staff who handle it can be considerable.[3] Under Article 28.4 the State Intelligence Agency will be responsible for issuing the Security Clearance of officials with access to confidential material. Too broad a definition of 'confidential' will mean that the SIA will be diverted from more important work simply to fulfil unnecessary security clearance requests. The same is true of the responsibility of Heads of Department to give security clearance to officials handling limited confidentiality classified information. In both cases there is also an attendant risk that large numbers of officials may be subject to official security vetting with intrusion into their personal lives and the handling and retention by the state of personal information concerning them in security files without there existing a pressing state interest. Concerns like these in the UK led in 1994 to a substantial reduction in the numbers of civil servants and government contractors requiring security clearance.

As currently drafted, the legislation catches within the net of criminal liability too wide a range of information. In particular, information whose disclosure would merely *disrupt* the administration of the state, national resources and/or public order is classified as confidential and of limited confidentiality when its disclosure would disrupt the execution of tasks and functions of state bodies (Arts. 8 and 9). It is questionable whether either category is appropriately protected by criminal law at all. *Arguably state interests would be adequately protected if unauthorised disclosure of confidential and of limited confidentiality classified information were a disciplinary matter dealt with employment sanctions against the relevant official (as is also envisaged in Arts. 27-29), rather than by criminal liability*.

Absence of Public Interest and Other Defences

Generally speaking the draft legislation fails to recognise that some disclosures of official information serve the public interest. As *Johannesburg Principle 13* states:

Armed Forces, Geneva, 3–5 October 2002, http://www.dcaf.ch/news/Intelligence%20Oversight_051002/ws_papers/caparini.pdf. For a brief explanation of over-classification see Laurence Lustgarten and Ian Leigh, *In From the Cold. National Security and Parliamentary Democracy* (Oxford, UK: Clarendon Press, 1994), 111–113.

[3] For example, in the US, it was calculated that the costs of protecting America's classified information was about 5.6 billion USD in 1995: according to US Representative David Skaggs, available at the website of the Information Security Oversight Office website, www.archives.gov/isoo.

Public Interest in Disclosure

In all laws and decisions concerning the right to obtain information, the public interest in knowing the information shall be a primary consideration.

Legislation across the globe protects the position of whistle-blowers in making public-spirited disclosures to expose governmental corruption and illegality by officials – see, for example, in the UK the Public Interest Disclosure Act 1998.[4] The position of whistleblowers is recognised in *Johannesburg Principle 16* which states

No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.

The absence of such a defence in the draft legislation is regrettable since it means that prosecutions may be undertaken even where the disclosure is a disinterested one designed to further accountability and the maintenance of the rule of law.

More broadly, there is no regard to the public interest in accountability in the terms that offences under the draft legislation are defined. This contravenes *Johannesburg Principle 15*, which states

No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

Once protected information has become public the justification for imposing criminal liability for its disclosure on a second or subsequent occasion disappears since any damage resulting from the disclosure has already occurred. However, under the draft Act there is no prior disclosure defence. To the contrary, Article 19 states: "A state secret's retention period shall not end in the event of its leakage," from which it follows that further disclosure remains an offence. This clearly contravenes *Johannesburg Principle 17*:

Information in the Public Domain

Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know.

4 www.opsi.gov.uk/acts/acts1998/ukpga_19980023_en_1.

Specific defences should be incorporated to recognise when the disclosure of information is in the public interest and when the information disclosed has already lost the quality of secrecy through prior publication.

Potential Liability of Journalists and Corporations

As noted above, the Act will apply to journalist as well as to officials. Under the draft Act, journalists and others who intentionally receive information covered by the legislation are liable under Art 45. Receiving information can be in essence involuntary – as, for example, where an email or letter is delivered to the recipient. In such cases presumably the defendant would be able to show that they did not intend to receive the information. In other cases, however, someone may intentionally accept delivery of an item while being unaware of the contents. The sense of the translation of the draft Act is unclear (particularly the reference to "should have knowledge of classified information"). *It is proposed that there should be a clearly-worded defence where the defendant was not aware of the nature of material that he received*.

By contrast, the UK Official Secrets Act targets the *further disclosure* of protected information by a journalist, rather than the mere receipt of the information in the first place (see s. 5 Official Secrets Act 1989, in particular s. 5(3)). This is perhaps a preferable approach. It would still leave open the possibility that where B (a journalist) agrees with A (an official) that A will pass information to B then B could be jointly charged with A of conspiracy to commit the offence, or counselling or procuring commission.

It appears from Art. 48 that a corporation may be liable because of criminal acts committed by those who "act for and on behalf of" the corporation or its interests. This is over-broad, since the acts in question may be unauthorised and/or without the knowledge of the company's management. In these circumstances it would be unjust to impute to the company the criminal intention of a rogue employee. The potential to levy very large fines ranging from fifty to one hundred billion rupiah on corporations convicted to offences (Art. 49.1) amounts to a substantial impediment of free speech. The scale of the penalties suggests that the intention behind the draft legislation is to intimidate news corporations to prevent them from reporting on anything approaching governmental secrecy, with a corresponding chilling effect on freedom of expression.

The power under Art. 49.2 to place corporations under supervision, suspend them, revoke their license or bar them from operations is clear infringement of press freedom, is also disproportionate and is open to obvious abuse as a means of intimidating a newspapers and broadcasters. *It is proposed that liability of cor-*

porations should be limited to situations in which someone who was the alter ego of the corporation (such as a director) has committed an offence and that the scale of penalties against corporations be substantially reduced, so as not to chill free speech.

Excessive Penalties

The *least serious* offence under the legislation incurs a penalty of a *minimum* of 5 years imprisonment ***and*** a *minimum* fine of 250,000,000 rupiah. Even at this level the scale of the fine is so greatly in excess of average incomes that it is presumably intended to not merely wipe out the entire assets of a convicted defendant but also to leave his or her family in poverty. It is not clear to me what happens within the Indonesian legal system when a defendant is unable to pay a court fine; for example, is an additional term of imprisonment imposed? The availability of the death penalty under Arts 44.3, Art. 45.3 and Arts. 46.3 for disclosures in wartime disregards the emerging consensus of civilised nations.

Johannesburg Principle 24: Disproportionate Punishments states that:

> A person, media outlet, political or other organization may not be subject to such sanctions, restraints or penalties for a security-related crime involving freedom of expression or information that are disproportionate to the seriousness of the actual crime.

The punishments imposed by this legislation are so severe as to clearly breach that principle. They should be reduced to more adequately reflect the range of damage that may result from result from disclosure of state secrets.

Appendix 1. The Johannesburg Principles

Principle 1: Freedom of Opinion, Expression and Information

(a) Everyone has the right to hold opinions without interference.

(b) Everyone has the right to freedom of expression, which includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his or her choice.

(c) The exercise of the rights provided for in paragraph (b) may be subject to restrictions on specific grounds, as established in international law, including for the protection of national security.

(d) No restriction on freedom of expression or information on the ground of national security may be imposed unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest. The burden of demonstrating the validity of the restriction rests with the government.

Principle 1.1: Prescribed by Law

(a) Any restriction on expression or information must be prescribed by law. The law must be accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to foresee whether a particular action is unlawful.

(b) The law should provide for adequate safeguards against abuse, including prompt, full and effective judicial scrutiny of the validity of the restriction by an independent court or tribunal.

Principle 1.2: Protection of a Legitimate National Security Interest

Any restriction on expression or information that a government seeks to justify on grounds of national security must have the genuine purpose and demonstrable effect of protecting a legitimate national security interest.

Principle 1.3: Necessary in a Democratic Society

To establish that a restriction on freedom of expression or information is necessary to protect a legitimate national security interest, a government must demonstrate that:

a) the expression or information at issue poses a serious threat to a legitimate national security interest;

b) the restriction imposed is the least restrictive means possible for protecting that interest; and

c) the restriction is compatible with democratic principles.

Principle 2: Legitimate National Security Interest

(a) A restriction sought to be justified on the ground of national security is not legiti-

mate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.

(b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

Principle 3: States of Emergency

In time of public emergency which threatens the life of the country and the existence of which is officially and lawfully proclaimed in accordance with both national and international law, a state may impose restrictions on freedom of expression and information but only to the extent strictly required by the exigencies of the situation and only when and for so long as they are not inconsistent with the government's other obligations under international law.

Principle 4: Prohibition of Discrimination

In no case may a restriction on freedom of expression or information, including on the ground of national security, involve discrimination based on race, colour, sex, language, religion, political or other opinion, national or social origin, nationality, property, birth or other status.

II. RESTRICTIONS ON FREEDOM OF EXPRESSION

Principle 5: Protection of Opinion

No one may be subjected to any sort of restraint, disadvantage or sanction because of his or her opinions or beliefs.

Principle 6: Expression That May Threaten National Security

Subject to Principles 15 and 16, expression may be punished as a threat to national security only if a government can demonstrate that:

a) the expression is intended to incite imminent violence;

b) it is likely to incite such violence; and

c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

Principle 7: Protected Expression

(a) Subject to Principles 15 and 16, the peaceful exercise of the right to freedom of expression shall not be considered a threat to national security or subjected to any

restrictions or penalties. Expression which shall not constitute a threat to national security includes, but is not limited to, expression that:

(i) advocates non-violent change of government policy or the government itself;

(ii) constitutes criticism of, or insult to, the nation, the state or its symbols, the government, its agencies, or public officials, or a foreign nation, state or its symbols, government, agencies or public officials;

(iii) constitutes objection, or advocacy of objection, on grounds of religion, conscience or belief, to military conscription or service, a particular conflict, or the threat or use of force to settle international disputes;

(iv) is directed at communicating information about alleged violations of international human rights standards or international humanitarian law.

(b) No one may be punished for criticizing or insulting the nation, the state or its symbols, the government, its agencies, or public officials, or a foreign nation, state or its symbols, government, agency.

Expression, whether written or oral, can never be prohibited on the ground that it is in a particular language, especially the language of a national minority.

Principle 10: Unlawful Interference With Expression by Third Parties

Governments are obliged to take reasonable measures to prevent private groups or individuals from interfering unlawfully with the peaceful exercise of freedom of expression, even where the expression is critical of the government or its policies. In particular, governments are obliged to condemn unlawful actions aimed at silencing freedom of expression, and to investigate and bring to justice those responsible.

III. RESTRICTIONS ON FREEDOM OF INFORMATION

Principle 11: General Rule on Access to Information

Everyone has the right to obtain information from public authorities, including information relating to national security. No restriction on this right may be imposed on the ground of national security unless the government can demonstrate that the restriction is prescribed by law and is necessary in a democratic society to protect a legitimate national security interest.

Principle 12: Narrow Designation of Security Exemption

A state may not categorically deny access to all information related to national security, but must designate in law only those specific and narrow categories of information that it is necessary to withhold in order to protect a legitimate national security interest.

Principle 13: Public Interest in Disclosure

In all laws and decisions concerning the right to obtain information, the public interest in knowing the information shall be a primary consideration.

Principle 14: Right to Independent Review of Denial of Information

The state is obliged to adopt appropriate measures to give effect to the right to obtain information. These measures shall require the authorities, if they deny a request for information, to specify their reasons for doing so in writing and as soon as reasonably possible; and shall provide for a right of review of the merits and the validity of the denial by an independent authority, including some form of judicial review of the legality of the denial. The reviewing authority must have the right to examine the information withheld.

Principle 15: General Rule on Disclosure of Secret Information

No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

Principle 16: Information Obtained Through Public Service

No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.

Principle 17: Information in the Public Domain

Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know.

Principle 18: Protection of Journalists' Sources

Protection of national security may not be used as a reason to compel a journalist to reveal a confidential source.

Principle 19: Access to Restricted Areas

Any restriction on the free flow of information may not be of such a nature as to thwart the purposes of human rights and humanitarian law. In particular, governments may not prevent journalists or representatives of intergovernmental or non-governmental organizations with a mandate to monitor adherence to human rights or humanitarian standards from entering areas where there are reasonable grounds to believe that violations of human rights or humanitarian law are being, or have been, committed. Governments may not exclude journalists or representatives of such organizations from areas that are experiencing violence or armed conflict except where their presence poses a clear risk to the safety of others.

IV. RULE OF LAW AND OTHER MATTERS

Principle 20: General Rule of Law Protections

Any person accused of a security-related crime involving expression or information is

entitled to all of the rule of law protections that are part of international law. These include, but are not limited to, the following rights:

a) the right to be presumed innocent;
b) the right not to be arbitrarily detained;
c) the right to be informed promptly in a language the person can understand of the charges and the supporting evidence against him or her;
d) the right to prompt access to counsel of choice;
e) the right to a trial within a reasonable time;
f) the right to have adequate time to prepare his or her defence;
g) the right to a fair and public trial by an independent and impartial court or tribunal;
h) the right to examine prosecution witnesses;
i) the right not to have evidence introduced at trial unless it has been disclosed to the accused and he or she has had an opportunity to rebut it; and
j) the right to appeal to an independent court or tribunal with power to review the decision on law and facts and set it aside.

Principle 21: Remedies

All remedies, including special ones, such as habeas corpus or amparo, shall be available to persons charged with security-related crimes, including during public emergencies which threaten the life of the country, as defined in Principle 3.

Principle 22: Right to Trial by an Independent Tribunal

(a) At the option of the accused, a criminal prosecution of a security-related crime should be tried by a jury where that institution exists or else by judges who are genuinely independent. The trial of persons accused of security-related crimes by judges without security of tenure constitutes a prima facie violation of the right to be tried by an independent tribunal.
(b) In no case may a civilian be tried for a security-related crime by a military court or tribunal.
(c) In no case may a civilian or member of the military be tried by an ad hoc or specially constituted national court or tribunal.

Principle 23: Prior Censorship

Expression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country under the conditions stated in Principle 3.

Principle 24: Disproportionate Punishments

A person, media outlet, political or other organization may not be subject to such sanc-

tions, restraints or penalties for a security-related crime involving freedom of expression or information that are disproportionate to the seriousness of the actual crime.

Principle 25: Relation of These Principles to Other Standards

Nothing in these Principles may be interpreted as restricting or limiting any human rights or freedoms recognized in international, regional or national law or standards.

Appendix 2. UK Official Secrets Act 1989

Chapter 6

An Act to replace section 2 of the Official Secrets Act 1911 by provisions protecting more limited classes of official information.
[11th May 1989]

Be it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

1. Security and Intelligence

(1) A person who is or has been—

a) a member of the security and intelligence services; or

b) a person notified that he is subject to the provisions of this subsection,

is guilty of an offence if without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services or in the course of his work while the notification is or was in force.

(2) The reference in subsection (1) above to disclosing information relating to security or intelligence includes a reference to making any statement which purports to be a disclosure of such information or is intended to be taken by those to whom it is addressed as being such a disclosure.

(3) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as such but otherwise than as mentioned in subsection (1) above.

(4) For the purposes of subsection (3) above a disclosure is damaging if—

a) it causes damage to the work of, or of any part of, the security and intelligence services; or

b) it is of information or a document or other article which is such that its unauthor-

ised disclosure would be likely to cause such damage or which falls within a class or description of information, documents or articles the unauthorised disclosure of which would be likely to have that effect.

(5) It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question related to security or intelligence or, in the case of an offence under subsection (3), that the disclosure would be damaging within the meaning of that subsection.

(6) Notification that a person is subject to subsection (1) above shall be effected by a notice in writing served on him by a Minister of the Crown; and such a notice may be served if, in the Minister's opinion, the work undertaken by the person in question is or includes work connected with the security and intelligence services and its nature is such that the interests of national security require that he should be subject to the provisions of that subsection.

(7) Subject to subsection (8) below, a notification for the purposes of subsection (1) above shall be in force for the period of five years beginning with the day on which it is served but may be renewed by further notices under subsection (6) above for periods of five years at a time.

(8) A notification for the purposes of subsection (1) above may at any time be revoked by a further notice in writing served by the Minister on the person concerned; and the Minister shall serve such a further notice as soon as, in his opinion, the work undertaken by that person ceases to be such as is mentioned in subsection (6) above.

(9) In this section "security or intelligence" means the work of, or in support of, the security and intelligence services or any part of them, and references to information relating to security or intelligence include references to information held or transmitted by those services or by persons in support of, or of any part of, them.

2. Defence

(1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to defence which is or has been in his possession by virtue of his position as such.

(2) For the purposes of subsection (1) above a disclosure is damaging if—

a) it damages the capability of, or of any part of, the armed forces of the Crown to carry out their tasks or leads to loss of life or injury to members of those forces or serious damage to the equipment or installations of those forces; or

b) otherwise than as mentioned in paragraph (a) above, it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citi-

zens abroad; or

c) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

(3) It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question related to defence or that its disclosure would be damaging within the meaning of subsection (1) above.

(4) In this section "defence" means—

a) the size, shape, organisation, logistics, order of battle, deployment, operations, state of readiness and training of the armed forces of the Crown;

b) the weapons, stores or other equipment of those forces and the invention, development, production and operation of such equipment and research relating to it;

c) defence policy and strategy and military planning and intelligence;

d) plans and measures for the maintenance of essential supplies and services that are or would be needed in time of war.

3. International Relations

(1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of—

a) any information, document or other article relating to international relations; or

b) any confidential information, document or other article which was obtained from a State other than the United Kingdom or an international organisation,

being information or a document or article which is or has been in his possession by virtue of his position as a Crown servant or government contractor.

(2) For the purposes of subsection (1) above a disclosure is damaging if—

a) it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad; or

b) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

(3) In the case of information or a document or article within subsection (1)(b) above—

a) the fact that it is confidential, or

b) its nature or contents,

may be sufficient to establish for the purposes of subsection (2)(b) above that the information, document or article is such that its unauthorised disclosure would be likely to have any of the effects there mentioned.

(4) It is a defence for a person charged with an offence under this section to prove that

at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question was such as is mentioned in subsection (1) above or that its disclosure would be damaging within the meaning of that subsection.

(5) In this section "international relations" means the relations between States, between international organisations or between one or more States and one or more such organisations and includes any matter relating to a State other than the United Kingdom or to an international organisation which is capable of affecting the relations of the United Kingdom with another State or with an international organisation.

(6) For the purposes of this section any information, document or article obtained from a State or organisation is confidential at any time while the terms on which it was obtained require it to be held in confidence or while the circumstances in which it was obtained make it reasonable for the State or organisation to expect that it would be so held.

4. Crime and Special Investigation Powers

(1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he discloses any information, document or other article to which this section applies and which is or has been in his possession by virtue of his position as such.

(2) This section applies to any information, document or other article—

a) the disclosure of which—

(i) results in the commission of an offence; or

(ii) facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody; or

(iii) impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders; or

b) which is such that its unauthorised disclosure would be likely to have any of those effects.

(3) This section also applies to—

a) any information obtained by reason of the interception of any communication in obedience to a warrant issued under section 2 of the [1985 c. 56.] Interception of Communications Act 1985, any information relating to the obtaining of information by reason of any such interception and any document or other article which is or has been used or held for use in, or has been obtained by reason of, any such interception; and

b) any information obtained by reason of action authorised by a warrant issued under section 3 of the [1989 c. 5.] Security Service Act 1989, any information relating to the obtaining of information by reason of any such action and any

document or other article which is or has been used or held for use in, or has been obtained by reason of, any such action.

(4) It is a defence for a person charged with an offence under this section in respect of a disclosure falling within subsection (2)(a) above to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the disclosure would have any of the effects there mentioned.

(5) It is a defence for a person charged with an offence under this section in respect of any other disclosure to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question was information or a document or article to which this section applies.

(6) In this section "legal custody" includes detention in pursuance of any enactment or any instrument made under an enactment.

5. Information Resulting from Unauthorised Disclosures or Entrusted in Confidence

(1) Subsection (2) below applies where—

a) any information, document or other article protected against disclosure by the foregoing provisions of this Act has come into a person's possession as a result of having been—

(i) disclosed (whether to him or another) by a Crown servant or government contractor without lawful authority; or

(ii) entrusted to him by a Crown servant or government contractor on terms requiring it to be held in confidence or in circumstances in which the Crown servant or government contractor could reasonably expect that it would be so held; or

(iii) disclosed (whether to him or another) without lawful authority by a person to whom it was entrusted as mentioned in sub-paragraph (ii) above; and

b) the disclosure without lawful authority of the information, document or article by the person into whose possession it has come is not an offence under any of those provisions.

(2) Subject to subsections (3) and (4) below, the person into whose possession the information, document or article has come is guilty of an offence if he discloses it without lawful authority knowing, or having reasonable cause to believe, that it is protected against disclosure by the foregoing provisions of this Act and that it has come into his possession as mentioned in subsection (1) above.

(3) In the case of information or a document or article protected against disclosure by sections 1 to 3 above, a person does not commit an offence under subsection (2) above unless—

a) the disclosure by him is damaging; and

b) he makes it knowing, or having reasonable cause to believe, that it would be damaging;

and the question whether a disclosure is damaging shall be determined for the purposes of this subsection as it would be in relation to a disclosure of that information, document or article by a Crown servant in contravention of section 1(3), 2(1) or 3(1) above.

(4) A person does not commit an offence under subsection (2) above in respect of information or a document or other article which has come into his possession as a result of having been disclosed—

a) as mentioned in subsection (1)(a)(i) above by a government contractor; or

b) as mentioned in subsection (1)(a)(iii) above,

unless that disclosure was by a British citizen or took place in the United Kingdom, in any of the Channel Islands or in the Isle of Man or a colony.

(5) For the purposes of this section information or a document or article is protected against disclosure by the foregoing provisions of this Act if—

a) it relates to security or intelligence, defence or international relations within the meaning of section 1, 2 or 3 above or is such as is mentioned in section 3(1)(b) above; or

b) it is information or a document or article to which section 4 above applies;

and information or a document or article is protected against disclosure by sections 1 to 3 above if it falls within paragraph (a) above.

(6) A person is guilty of an offence if without lawful authority he discloses any information, document or other article which he knows, or has reasonable cause to believe, to have come into his possession as a result of a contravention of section 1 of the [1911 c. 28.] Official Secrets Act 1911.

6. Information Entrusted in Confidence to Other States or International Organisations

(1) This section applies where—

a) any information, document or other article which—

(i) relates to security or intelligence, defence or international relations; and

(ii) has been communicated in confidence by or on behalf of the United Kingdom to another State or to an international organisation,

has come into a person's possession as a result of having been disclosed (whether to him or another) without the authority of that State or organisation or, in the case of an organisation, of a member of it; and

b) the disclosure without lawful authority of the information, document or article by

the person into whose possession it has come is not an offence under any of the foregoing provisions of this Act.

(2) Subject to subsection (3) below, the person into whose possession the information, document or article has come is guilty of an offence if he makes a damaging disclosure of it knowing, or having reasonable cause to believe, that it is such as is mentioned in subsection (1) above, that it has come into his possession as there mentioned and that its disclosure would be damaging.

(3) A person does not commit an offence under subsection (2) above if the information, document or article is disclosed by him with lawful authority or has previously been made available to the public with the authority of the State or organisation concerned or, in the case of an organisation, of a member of it.

(4) For the purposes of this section "security or intelligence," "defence" and "international relations" have the same meaning as in sections 1, 2 and 3 above and the question whether a disclosure is damaging shall be determined as it would be in relation to a disclosure of the information, document or article in question by a Crown servant in contravention of section 1(3), 2(1) and 3(1) above.

(5) For the purposes of this section information or a document or article is communicated in confidence if it is communicated on terms requiring it to be held in confidence or in circumstances in which the person communicating it could reasonably expect that it would be so held.

7. Authorised Disclosures

(1) For the purposes of this Act a disclosure by—

a) a Crown servant; or

b) a person, not being a Crown servant or government contractor, in whose case a notification for the purposes of section 1(1) above is in force,

is made with lawful authority if, and only if, it is made in accordance with his official duty.

(2) For the purposes of this Act a disclosure by a government contractor is made with lawful authority if, and only if, it is made—

a) in accordance with an official authorisation; or

b) for the purposes of the functions by virtue of which he is a government contractor and without contravening an official restriction.

(3) For the purposes of this Act a disclosure made by any other person is made with lawful authority if, and only if, it is made—

a) to a Crown servant for the purposes of his functions as such; or

b) in accordance with an official authorisation.

(4) It is a defence for a person charged with an offence under any of the foregoing provisions of this Act to prove that at the time of the alleged offence he believed that

he had lawful authority to make the disclosure in question and had no reasonable cause to believe otherwise.

(5) In this section "official authorisation" and "official restriction" mean, subject to subsection (6) below, an authorisation or restriction duly given or imposed by a Crown servant or government contractor or by or on behalf of a prescribed body or a body of a prescribed class.

(6) In relation to section 6 above "official authorisation" includes an authorisation duly given by or on behalf of the State or organisation concerned or, in the case of an organisation, a member of it.

8. Safeguarding of Information

(1) Where a Crown servant or government contractor, by virtue of his position as such, has in his possession or under his control any document or other article which it would be an offence under any of the foregoing provisions of this Act for him to disclose without lawful authority he is guilty of an offence if—

a) being a Crown servant, he retains the document or article contrary to his official duty; or

b) being a government contractor, he fails to comply with an official direction for the return or disposal of the document or article,

or if he fails to take such care to prevent the unauthorised disclosure of the document or article as a person in his position may reasonably be expected to take.

(2) It is a defence for a Crown servant charged with an offence under subsection (1)(a) above to prove that at the time of the alleged offence he believed that he was acting in accordance with his official duty and had no reasonable cause to believe otherwise.

(3) In subsections (1) and (2) above references to a Crown servant include any person, not being a Crown servant or government contractor, in whose case a notification for the purposes of section 1(1) above is in force.

(4) Where a person has in his possession or under his control any document or other article which it would be an offence under section 5 above for him to disclose without lawful authority, he is guilty of an offence if—

a) he fails to comply with an official direction for its return or disposal; or

b) where he obtained it from a Crown servant or government contractor on terms requiring it to be held in confidence or in circumstances in which that servant or contractor could reasonably expect that it would be so held, he fails to take such care to prevent its unauthorised disclosure as a person in his position may reasonably be expected to take.

(5) Where a person has in his possession or under his control any document or other article which it would be an offence under section 6 above for him to disclose without lawful authority, he is guilty of an offence if he fails to comply with an official di-

rection for its return or disposal.

(6) A person is guilty of an offence if he discloses any official information, document or other article which can be used for the purpose of obtaining access to any information, document or other article protected against disclosure by the foregoing provisions of this Act and the circumstances in which it is disclosed are such that it would be reasonable to expect that it might be used for that purpose without authority.

(7) For the purposes of subsection (6) above a person discloses information or a document or article which is official if—

a) he has or has had it in his possession by virtue of his position as a Crown servant or government contractor; or

b) he knows or has reasonable cause to believe that a Crown servant or government contractor has or has had it in his possession by virtue of his position as such.

(8) Subsection (5) of section 5 above applies for the purposes of subsection (6) above as it applies for the purposes of that section.

(9) In this section "official direction" means a direction duly given by a Crown servant or government contractor or by or on behalf of a prescribed body or a body of a prescribed class.

9. Prosecutions

(1) Subject to subsection (2) below, no prosecution for an offence under this Act shall be instituted in England and Wales or in Northern Ireland except by or with the consent of the Attorney General or, as the case may be, the Attorney General for Northern Ireland.

(2) Subsection (1) above does not apply to an offence in respect of any such information, document or article as is mentioned in section 4(2) above but no prosecution for such an offence shall be instituted in England and Wales or in Northern Ireland except by or with the consent of the Director of Public Prosecutions or, as the case may be, the Director of Public Prosecutions for Northern Ireland.

10. Penalties

(1) A person guilty of an offence under any provision of this Act other than section 8(1), (4) or (5) shall be liable—

a) on conviction on indictment, to imprisonment for a term not exceeding two years or a fine or both;

b) on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or both.

(2) A person guilty of an offence under section 8(1), (4) or (5) above shall be liable on summary conviction to imprisonment for a term not exceeding three months or a

fine not exceeding level 5 on the standard scale or both.

11. Arrest, Search and Trial

(1) In section 24(2) of the [1984 c. 60] Police and Criminal Evidence Act 1984 (arrestable offences) in paragraph (b) for the words "the Official Secrets Acts 1911 and 1920" there shall be substituted the words "the Official Secrets Act 1920" and after that paragraph there shall be inserted—

"(bb) offences under any provision of the Official Secrets Act 1989 except section 8(1), (4) or (5);"

(2) Offences under any provision of this Act other than section 8(1), (4) or (5) and attempts to commit them shall be arrestable offences within the meaning of section 2 of the [1967 c. 18 (N.I.)] Criminal Law Act (Northern Ireland) 1967.

(3) Section 9(1) of the [1911 c. 28] Official Secrets Act 1911 (search warrants) shall have effect as if references to offences under that Act included references to offences under any provision of this Act other than section 8(1), (4) or (5); and the following provisions of the Police and Criminal Evidence Act 1984, that is to say—

a) section 9(2) (which excludes items subject to legal privilege and certain other material from powers of search conferred by previous enactments); and

b) paragraph 3(b) of Schedule 1 (which prescribes access conditions for the special procedure laid down in that Schedule),

shall apply to section 9(1) of the said Act of 1911 as extended by this subsection as they apply to that section as originally enacted.

(4) Section 8(4) of the [1920 c. 75.] Official Secrets Act 1920 (exclusion of public from hearing on grounds of national safety) shall have effect as if references to offences under that Act included references to offences under any provision of this Act other than section 8(1), (4) or (5).

(5) Proceedings for an offence under this Act may be taken in any place in the United Kingdom.

12. "Crown Servant" and "Government Contractor"

(1) In this Act "Crown servant" means—

a) a Minister of the Crown;

b) a person appointed under section 8 of the [1973 c. 36] Northern Ireland Constitution Act 1973 (the Northern Ireland Executive etc.);

c) any person employed in the civil service of the Crown, including Her Majesty's Diplomatic Service, Her Majesty's Overseas Civil Service, the civil service of Northern Ireland and the Northern Ireland Court Service;

d) any member of the naval, military or air forces of the Crown, including any person employed by an association established for the purposes of the [1980 c. 9]

Reserve Forces Act 1980;

e) any constable and any other person employed or appointed in or for the purposes of any police force (including a police force within the meaning of the [1970 c. 9 (N.I.)] Police Act (Northern Ireland) 1970);

f) any person who is a member or employee of a prescribed body or a body of a prescribed class and either is prescribed for the purposes of this paragraph or belongs to a prescribed class of members or employees of any such body;

g) any person who is the holder of a prescribed office or who is an employee of such a holder and either is prescribed for the purposes of this paragraph or belongs to a prescribed class of such employees.

(2) In this Act "government contractor" means, subject to subsection (3) below, any person who is not a Crown servant but who provides, or is employed in the provision of, goods or services—

a) for the purposes of any Minister or person mentioned in paragraph (a) or (b) of subsection (1) above, of any of the services, forces or bodies mentioned in that subsection or of the holder of any office prescribed under that subsection; or

b) under an agreement or arrangement certified by the Secretary of State as being one to which the government of a State other than the United Kingdom or an international organisation is a party or which is subordinate to, or made for the purposes of implementing, any such agreement or arrangement.

(3) Where an employee or class of employees of any body, or of any holder of an office, is prescribed by an order made for the purposes of subsection (1) above—

a) any employee of that body, or of the holder of that office, who is not prescribed or is not within the prescribed class; and

b) any person who does not provide, or is not employed in the provision of, goods or services for the purposes of the performance of those functions of the body or the holder of the office in connection with which the employee or prescribed class of employees is engaged,

shall not be a government contractor for the purposes of this Act.

13. Other Interpretation Provisions

(1) In this Act—

- "disclose" and "disclosure," in relation to a document or other article, include parting with possession of it;
- "international organisation" means, subject to subsections (2) and (3) below, an organisation of which only States are members and includes a reference to any organ of such an organisation;
- "prescribed" means prescribed by an order made by the Secretary of State;
- "State" includes the government of a State and any organ of its government and

references to a State other than the United Kingdom include references to any territory outside the United Kingdom.

(2) In section 12(2)(b) above the reference to an international organisation includes a reference to any such organisation whether or not one of which only States are members and includes a commercial organisation.

(3) In determining for the purposes of subsection (1) above whether only States are members of an organisation, any member which is itself an organisation of which only States are members, or which is an organ of such an organisation, shall be treated as a State.

14. Orders

(1) Any power of the Secretary of State under this Act to make orders shall be exercisable by statutory instrument.

(2) No order shall be made by him for the purposes of section 7(5), 8(9) or 12 above unless a draft of it has been laid before, and approved by a resolution of, each House of Parliament.

(3) If, apart from the provisions of this subsection, the draft of an order under any of the provisions mentioned in subsection (2) above would be treated for the purposes of the Standing Orders of either House of Parliament as a hybrid instrument it shall proceed in that House as if it were not such an instrument.

15. Acts Done Abroad and Extent

(1) Any act—

a) done by a British citizen or Crown servant; or

b) done by any person in any of the Channel Islands or the Isle of Man or any colony,

shall, if it would be an offence by that person under any provision of this Act other than section 8(1), (4) or (5) when done by him in the United Kingdom, be an offence under that provision.

(2) This Act extends to Northern Ireland.

(3) Her Majesty may by Order in Council provide that any provision of this Act shall extend, with such exceptions, adaptations and modifications as may be specified in the Order, to any of the Channel Islands or the Isle of Man or any colony.

16. Short Title, Citation, Consequential Amendments, Repeals, Revocation and Commencement

(1) This Act may be cited as the Official Secrets Act 1989.

(2) This Act and the Official Secrets Acts 1911 to 1939 may be cited together as the Official Secrets Acts 1911 to 1989.

(3) Schedule 1 to this Act shall have effect for making amendments consequential on

the provisions of this Act.

(4) The enactments and Order mentioned in Schedule 2 to this Act are hereby repealed or revoked to the extent specified in the third column of that Schedule.

(5) Subject to any Order under subsection (3) of section 15 above the repeals in the Official Secrets Act 1911 and the Official Secrets Act 1920 do not extend to any of the territories mentioned in that subsection.

Indonesian Draft Law on State Secrets

Peter Gill

Introduction

As a general principle, in a democratic society the *presumption* should be that information in the possession of the state should be available to citizens since that access provides the means by which informed debates about public policy can take place and without which citizens will not have the tools by which they can hold the government to account. I have used primarily UK experience to draw comparisons with the Indonesian draft law but it must be noted that, among the 'old democracies,' the UK has a justly earned reputation as being highly secretive. There is a long history of secrecy legislation back to the late nineteenth century but it is only in the last ten years that the UK has adopted freedom of information legislation granting a right to citizens to access government information. Of course, there are exemptions to that, including material relating to security, law enforcement, personal privacy etc. but there is also a robust Information Commissioner who is empowered to challenge government decisions not to release information (www.ico.gov.uk).

The Indonesian draft state secrets law is based on the *presumption* that wide classes of information will be secret at the discretion of the President or nominees and the threshold of 'harm' for determining what is secret is so low as to inhibit normal exchange of information and political activity. This is shown in more detail below. Ideally, this law would be examined together with the Freedom of Information Act passed in 2008 and to be brought into effect in 2010 since the issues are two sides of the same coin. However, in the time available, I have not attempted to do that systematically. In some places the draft secrets law seems rather vague or hard to follow; I realise this may be because of problems in translation. Similarly, apologies if my comments below are inappropriate because I have misunderstood the meaning of specific provisions. Extracts from the draft secrets law and the UK Official Secrets Acts (OSA) are highlighted by being placed in boxes.

Coverage of the Law

Article 1

Under this law, what is referred to as:

1. State Secrets are information, objects and/or activities officially determined by the President that should be kept confidential for due protection according to the management standard and procedure; which upon knowledge of ineligible persons may be injurious to the sovereignty, integrity and safety of the Unitary State of the Republic of Indonesia and/or may result in disruptions to the administration of the state, national resources, public order and/or to the execution of the tasks and functions of state bodies.

The intended breadth of the law is excessive, especially if article 6.b. is the 'catch-all' provision it looks like (see below). State secrets are any information etc. that the President deems would, if disclosed, injure national sovereignty and safety and/or disrupt public administration. Defending national sovereignty and safety would be found in all national laws but guarding against 'disruptions' is unusually broad. 'Disruption' is defined in the Concise English Dictionary as 'disturb or interrupt': the exchange of information leading to the 'disturbance' of public administration may certainly be *inconvenient* for state officials but it should not be the object of such draconian law. Criticism of public administration is the lifeblood of democracy.

Article 3 refers to information, objects and/or facilities, and activities as 'types of state secrets' and Article 6 seems to limit the coverage of the Law to:

a. Information consists of the following:
   1) Information related to state defense
   2) Information related to TNI mobilization plans including its organizing and functions
   3) Information related to intelligence
   4) Information related to the state encryption system covering data and information on coding materials, encryption application method and technique, usage pattern as well as the search and analysis of the coded information of other parties including data and information on the coding materials used, search and analysis activities, encrypted information sources, analysis results and coding personnel
   5) Information related to foreign relations
   6) Information related to national economic resilience

But then, Article 6 ends with what looks like a 'catch-all' phrase to include potentially even more information:

> b) Type of other state secrets as stipulated in Article 3 exempted by the law and which brings about consequences as mentioned in Article 7, Article 8, and Article 9.

If it were intended that the Law should apply only to those six areas specified in 6.a. above (which would be desirable) then the Law would need to state that specifically; as it is, there appears to be no limit to the discretion of officials as to what may be deemed a state secret. Given the penalties in the law (see section 8 below) this would pose serious threat to freedoms of the press and speech. This was the situation in the UK where the Official Secrets Act 1911 s.2 was a similar 'catch-all' provision that, interpreted naturally, meant that no civil servant or government contractor could communicate to any other person any information, however trivial, without prior authorisation. This gave rise to many controversial cases, especially during the 1970s and 1980s in which the law was brought into disrepute. Since *any* commentary or reporting on government issues by journalists, researchers or citizens may be interpreted as involving *some* breach of the law, such 'catch-all' provisions make prosecution *possible* in many cases and leaves journalists and others in a position of much uncertainty. This leaves too much discretion with officials as to whether to *actually* prosecute (see section 6 below). This is not consistent with ideas of freedom of speech and press that are central to democratic societies.

As a result the Official Secrets Act 1989 was introduced in UK to replace OSA 1911, s.2 and limited the coverage of the criminal law to just six classes of information (similar to those above in Article 6.a.):

1. Security and intelligence
2. Defence
3. International relations
4. Crime and special investigation powers
5. Information resulting from unauthorised disclosures or entrusted in confidence
6. Information entrusted in confidence to other states or international organisations.

The 'Harm' Test

Article 6.a. in the draft secrets law lists many specific types of information as examples of state secrets (see above) and then articles 7-9 identify the test of 'harm' that is required so that secrets can be distinguished from information that can be released:

> **Article 7**
> State secret is categorized as highly confidential as stipulated in Article 5 point b, when such classified information is made known to ineligible parties and it jeopardizes the sovereignty of the state, territorial integrity of the Unitary State of the Republic of Indonesia and/or the security of the nation.

By comparison with countries elsewhere, the threshold of 'harm' in article 7 is very low (articles 8 and 9 are discussed below). 'Jeopardise' (article 7) is defined in the Concise Oxford Dictionary (COD) as 'put at risk of loss, harm or failure.' One might compare this with UK Official Secrets Act, 1989, s.2 on, for example, military matters:

> **2. Defence**
> (1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to defence which is or has been in his possession by virtue of his position as such.
> (2) For the purposes of subsection (1) above a disclosure is damaging if—
> a) it damages the capability of, or of any part of, the armed forces of the Crown to carry out their tasks or leads to loss of life or injury to members of those forces or serious damage to the equipment or installations of those forces; or
> b) otherwise than as mentioned in paragraph (a) above, it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom of those interests or endangers the safety of British citizens abroad; or
> c) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

Two points might be noted. First the UK law does not set out a long list of specific forms of information (as contained in draft law article 6.a.1). Second, the 'harm' threshold is higher: it refers to 'damage' which is defined in the COD as

'physical harm impairing the value, usefulness or normal function of…'; 'loss of life or injury…'; 'serious damage to equipment…'; 'seriously obstructs…'.

Article 6.a.(3) includes a long list of specifics that constitute state secrets with respect to intelligence. It might be suggested that such a list is unnecessary, for example, in the UK OSA 1989, s.1 simply refers to 'any information, document or other article…'.

> **1. Security and Intelligence**
>
> (1) A person who is or has been—
>
> a) a member of the security and intelligence services; or
>
> b) a person notified that he is subject to the provisions of this subsection,
>
> is guilty of an offence if without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services or in the course of his work while the notification is or was in force.

As it stands, some of the items specified in the draft would need to be protected, for example, identity of informants [6.a.(3)c)], products of covert surveillance [6.a.(3)e)], protective security information [6.a.(3)j)], but other sub-sections are too broad. For example, article 6.a.(3):

> f) Reports, information, statistics and other data on the operations of the intelligence agency.

Taken together with other articles in the draft law, 'other data' appears to criminalise the publication of *anything* about intelligence. Again, this should be linked to a harm test. Although UK OSA 1989, s.1 (above) also refers to the publication of 'any' information, it should be noted that in the context of greater freedom to information, the Security Service (MI5) now maintains its own web-site containing 'reports, information and statistics' on their operation.[1] There is a good deal of information even about intelligence agencies which can and should be published in order to educate the public about security policies and to increase the effectiveness and efficiency with which they operate. Great care must be taken not to criminalise all disclosures since, again, this may simply conceal financial corruption, inefficiency and the abuse of human rights.

---

[1] See www.mi5.gov.uk.

There is an apparent inconsistency within Article 6: whereas 6.a.(1)–(4) include no harm test, 6.a.(5)–(6) do.

Article 6.a.(5) includes as a state secret:

> b) Information and documents related to the political and military situation of other countries based on reasons that shall not be publicized and where their disclosure will be detrimental to the national security of the country in question.

This seems to be unnecessary, unenforceable and potentially dangerous to freedom of speech. It is accepted international practice within international relations and defence and intelligence co-operation that information supplied by one country to another is not released by the recipient without the permission of the donor (the so-called 'third party rule'). But the improper disclosure of this information would already be adequately covered by other articles in the draft law protecting the operations of the Indonesian government, for example, article 6.a.(5)a. Therefore it is not necessary to incorporate this custom in law in this way and it is not desirable since it might hinder perfectly legitimate commentary in Indonesia on the political or military situation in other countries.

Article 6, Information related to national economic resilience, includes:

> b) Research conducted by the Government with the objective to serve national economic interests.
> c) Information related to techniques, technology or solutions whereby their disclosure will be detrimental to national economic interests.

These must be linked specifically to a 'harm' test because research, whether carried out by government, in universities or in the corporate sector requires some degree of open debate between scholars and researchers. It would not serve Indonesian national interests in a globalised economy to have all this work treated as a state secret. Of course, there are risks attached to the free circulation of ideas and information but these risks cannot be completely eliminated other than in a highly authoritarian and closed society. In democratic societies the advantages of free and open circulation of research and ideas far outweigh the occasional costs of specific cases of, say, technology theft.

Articles 8 and 9 seek to protect against the improper disclosure of information that is something less than 'highly confidential' as covered in article 7.

Article 8

State secret is categorized as confidential as stipulated in Article 5 point b when such classified information is made known to ineligible parties and disrupts the administration of the state, national resources and/or public order.

Article 9

State secret is categorized as having limited confidentiality as stipulated in Article 5 point c when such classified information is made known to ineligible parties and disrupts the execution of tasks and functions of state bodies.

First, it may be that something has been lost in the translation of these articles into English, but it is not clear to me that there is any distinction between "the administration of the state" and "the execution of tasks and functions of state bodies." This will not provide officials with useful guidance in their making of classification decisions in the first place (as covered in chapters III and IV of the draft law). It is generally acknowledged that there is a tendency within bureaucracies to 'play safe' and over-classify information beyond what is strictly necessary on security grounds. That tendency is likely to be reinforced where there is little or no difference between categories.

Second, as in the argument above with regard to article 7, I would suggest that, by international standards, the 'harm' threshold in articles 8 and 9 is very low. 'Disrupts' means, according to the Concise Oxford Dictionary, 'disturb or interrupt.' Especially when these thresholds are considered in the light of proposed penalties, for example, minimum prison sentence of five years in the case of 'confidential' information (articles 44–46 – see further in section 8 below), the draft law looks to be disproportionately severe. Political opposition is central to the functioning of modern democratic states and legal opposition revolves around the critique both of the substance of government policies and the efficiency or otherwise of government administration. Clearly, such opposition may be viewed by government ministers and state officials as inconvenient, embarrassing or even 'disturbing' but such is the price of democratic freedom. The alternative risks the 'chilling' of opposition, dissent and the denial of journalistic and press freedom upon which healthy democracies depend.

I understand that the Freedom of Information legislation passed in 2008 envisages the establishment of independent public information commissions who would settle disputes between citizens and officials over the release of state information. These Commissions will be unable to operate in the core areas of intelligence, security, defence, foreign relations and economic competitiveness (which is unfortu-

nate) but their job will be very difficult in the other areas of state policy if state officials are able to rely on articles 8 and 9 of the State Secrets law as drafted here.

Management and Oversight

Article 23 legislates that:

> The Advisory Board for State Secret Policy shall carry out the task of formulating policies and ensuring the oversight of the proper administration of state secrets pursuant to Article 13 clause (2).

It is entirely appropriate that such a body be established to formulate policy and assume responsibility for oversight *internal* to the government but it should be noted that oversight also needs to be provided *externally*. In order to bring the Freedom of Information and State Secrets laws into a complementary relationship, one logical possibility would be to empower the FOI Commissions to provide this external oversight.

Burden of Proof and Defences

Article 34 refers to 'ineligible or unauthorized' people who come into possession of state secrets 'unintentionally' and their obligation to return the material to its rightful owner. This is presumably aimed at those who are not state officials with adequate clearance and therefore covers all citizens. The article is understandable but such people may have no reason to believe that the material is a state secret. They will not have been trained in the recognition and handling of secret material and therefore it would be unjust if, for example, they were criminally liable for a failure 'to preserve' the material. Therefore, this article should incorporate an additional sub-section to the effect that it would be a defence if the person had no reasonable cause to believe that the material or media was a state secret. Such a provision can be found in the UK OSA 1989 where it provides such a defence to state officials and contractors:

> **2. Defence**
>
> (1) A person who is or has been a Crown servant or government contractor is guilty of an offence if without lawful authority he makes a damaging disclosure of any information, document or other article relating to defence which is or has been in his possession by virtue of his position as such.
>
> …

(3) It is a defence for a person charged with an offence under this section to prove that at the time of the alleged offence he did not know, and had no reasonable cause to believe, that the information, document or article in question related to defence or that its disclosure would be damaging within the meaning of subsection (1) above.

Here we see that the burden of proof is on the official or contractor to prove that they did not know and had no reasonable cause to believe that the material was secret.

But for *citizens* who come into possession of state secrets (as apparently covered by article 34) the burden of proof should remain on the prosecution, for example, the UK OSA 1989 s.5 is equivalent to article 34:

5. Information Resulting from Unauthorised Disclosures or Entrusted in Confidence …

(2) Subject to subsections (3) and (4) below, the person into whose possession the information, document or article has come is guilty of an offence if he discloses it without lawful authority knowing, or having reasonable cause to believe, that it is protected against disclosure by the foregoing provisions of this Act and that it has come into his possession as mentioned in subsection (1) above.

(3) In the case of information or a document or article protected against disclosure by sections 1 to 3 above [security and intelligence, defence, international relations], a person does not commit an offence under subsection (2) above unless—

a) the disclosure by him is damaging; and

b) he makes it knowing, or having reasonable cause to believe, that it would be damaging; …

Consent to Prosecution

It has been shown that the draft secrets law provides wide discretion to officials to determine what are state secrets with no external oversight which provides great risk of infringing on democratic freedoms of press and speech. Cases involving state secrecy often engender major political controversy and, even if this wide discretion were to be narrowed before the final law is passed, it would still be desirable that a senior official is responsible for overseeing prosecutions. In the UK OSA 1989, for example, prosecutions require the approval of the Attorney General:

9. Prosecutions

(1) Subject to subsection (2) below, no prosecution for an offence under this Act shall be instituted in England and Wales or in Northern Ireland except by or with the consent of the Attorney General or, as the case may be, the Attorney General for Northern Ireland.

Secrecy and Due Process of Law

Articles 38 and 39 deal with the issue of court proceedings involving state secrets. All jurisdictions face the conundrum that criminal proceedings should take place in public and yet that might lead to the disclosure of the very state secrets that the law seeks to protect. Therefore all countries have procedures that seek to maximise the protection of state secrets and the requirement for open trials. Democracy and legal due process require that as much evidence as possible is presented openly. Article 38 does not meet this standard since it replaces 'state secrets' with 'an explanatory letter' even though article 41 provides for closed trials of criminal cases involving classified material. Together, these provisions raise the prospect of people being tried behind closed doors on the basis of evidence that is not produced, just 'explanatory letters' from the state body responsible for the protection of secrecy. In the UK similar proceedings have taken place under the Prevention of Terrorism Act 2005 with respect to the institution of 'control orders' against those suspected of involvement in terrorist activities but where there is neither sufficient evidence for a prosecution and, in the case of non-citizens, they cannot be deported because there is a realistic possibility that they would be tortured in their home country. However, this regime has been constantly criticised by the House of Lords because detainees are ignorant of the information upon which they are detained and therefore unable effectively to challenge it. Further court challenges are pending and it is believed likely that the control order regime will now lapse. Certainly, providing for similar procedures in legislation, as envisaged in the Indonesian draft law, would be considered unwise.

In more routine cases, the UK makes use of a procedure based on 'public interest immunity.' In essence, if the government or prosecution believes that revealing certain documents would cause damage then it may request that they be kept confidential by means of a minister signing a public interest immunity certificate. The judge will consider this in the light of representations from the defence and make a determination as to what may and may not be made available to the defence and also on other matters, for example, whether certain witnesses may appear anonymously and screened and whether certain parts of the evidence

should be heard in secret. The key difference between this procedure and that envisaged in articles 38-39 is that *the court* makes the final decision as to whether the public interest in secrecy outweighs the public interest in fair and open trials.

Penalties

The problem with such a low threshold of harm in the Indonesian draft law is reinforced by the vagueness of articles 44-46 and the severe penalties set out. For example:

> **Article 44**
>
> (1) Every person who with intent and in breach of the law to obtain and/or disseminate state secret classified as Highly Confidential to another party ineligible to have knowledge of such information is liable to punishment for a minimum of 7 (seven) years to a maximum of 20 (twenty) years imprisonment and a fine of at least Rp 50,000,000 (fifty million rupiah) to a maximum of Rp 1,000,000,000 (one billion rupiah).

This article refers to the potential for espionage ('obtain') and unlawful disclosure ('disseminate') but is vague on intent: 'with intent' to do what? It should be made clearer that the intent relates to the harm test. The problem otherwise can be illustrated by some examples from article 6; article 6.a.(1) includes as 'state secrets':

> f) Information related to the structural design, industrial tests and placement of defence forces on the latest armament prototype, combat technology, ammunition and mobilization capacity of the respective industry.
>
> g) Information related to preparations and support for the national general war plan including physical weaponry support, financial support, energy sources and regulatory instruments.

Okay, but what of the case where a journalist obtains information that new technologies are inefficient, that ammunition is defective or that financial support provided to the military by the government is inadequate to support existing war plans? In such cases, the 'intent' of an official in disclosing information or a journalist in publishing such information would not be to 'jeopardise… the security of the nation' (Article 7) but to expose corruption or inefficiency and it would clearly be in the national interest that such exposures were made. Therefore, the law

needs to make this clearer and might, for example, incorporate a 'public interest' in defence.

Similarly, article 6.a.(2) identifies as a state secret:

> d) Information related to high-ranking state officials as well as the government authorized and responsible for defense preparedness.

It is entirely proper if the law seeks to protect the lives of such officials but, again, any disclosure of information should be linked to a harm test such as 'loss of life or injury' as in the UK OSA 1989 s.2 referred to earlier. The current draft is too general and would appear to prevent, say, a journalist exposing corruption among officials. Such exposures are in, not against, the public interest.

Clearly, levels of punishment vary widely between countries and in line with national traditions but the contrast with those envisaged in the UK OSA 1989 is great:

> **10. Penalties**
>
> (1) A person guilty of an offence under any provision of this Act other than section 8(1), (4) or (5) shall be liable—
>
> a) on conviction on indictment, to imprisonment for a term not exceeding two years or a fine or both;
>
> b) on summary conviction, to imprisonment for a term not exceeding six months or a fine not exceeding the statutory maximum or both.

Indonesian Draft Law on State Secrets

Mindia Vashakmadze

Article I: General Provisions

The protection of state secrets must be balanced against the access to information, democratic accountability and fair trial guarantees. Excessive secrecy runs against these principles. According to international standards that are accepted in democratic states in Europe, the laws on state secrecy should not be overly broad. The Indonesian bill takes an opposite approach and covers a wide variety of issues that are not directly related to national security.

Categories of classified information cover not only state security but also the organization and tasks of the military, economy, and foreign policy. Under each category, there are a number of sub-categories. Many of these categories are not strictly limited to the national security area and may lead to substantial restrictions on access to information. Broad classification may facilitate a culture of government secrecy and damage the freedom of Information. For example, the information on foreign relations that is classified as state secrets is broad and this may put into question an effective democratic control of foreign policy. Moreover, an overbroad classification of information regarding the military institution may also endanger the ongoing reforms and public discussion on the changing patterns of civil-military relations in Indonesia.[1] The designation of classified information should not apply to such information unless it directly affects the national security of the nation. *Thus the law should set out narrow categories of information that can be classified as state secrets.* For example, the Estonian State Secrets Act sets out specifically each of the types of information that can be classified, under which category they can be classified, and for how long they can be classified.

[1] Article 15: General Rule on Disclosure of Secret Information "No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and it is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure," Johannesburg Principles on National Security, Freedom of Expression and Access to Information of 1995.

According to the bill, the harm to be prevented is not limited to state security – the release of classified information can damage the sovereignty, integrity, and safety of the Indonesian state and result in disruptions to the administration of the state, national resources, public order and to the execution of the tasks and functions of state bodies (Article 1.1). For example, information related to foreign relations policy plan and the corresponding tasks may be classified if their unauthorized disclosure will cause losses and damages to the *interests* of the state. Such broad formulations leave the space for misinterpretation. The bill should be more specific in that regard and set out the concept of harm in more specific terms.

Article II. State Secrecy as an Exclusive Prerogative of the Executive Power

The competencies of the President are broadly defined. The bill gives the President the powers related to the classification, administration and retention of state secrets (Article 11.1). These powers can be delegated to the head of the respective state agency. Furthermore, the President formulates the standard and procedure for the protection and management of state secrets (12.1). Additionally, authority on the administration of state secrets rests with the President (13.1). The law does not specify how these powers are implemented in practice. The President can delegate these powers to the respective state body.

However, the law does not specify the tasks of Parliament which, in a democratic society, is to issue all primary legislation on state secrecy and, furthermore, should develop state policy regarding state secrecy. Conferring wide-ranging powers on the President marks the exclusive governmental domination in this field.

The scope of parliamentary involvement in state secrecy policy-making should be strengthened. In many countries, the primary responsibility to define the fundamental principles on state secrecy and to issue legislation on this issues lies with the Parliament. For example, Article 3.1 of the Georgian Law on State Secrets states:

> The state policy regarding state secrets, as a component part of the policy for ensuring sovereignty, defence and national security of Georgia, shall be developed by the Parliament of Georgia.

Article III. Type and Level of Confidentiality

The draft differentiates between three levels of confidentiality: state secrets may be highly confidential, confidential and limited confidential. However, the level of harm to national security for all three categories is not formulated in such a way that would exclude any possibility of misinterpretation.

The disclosure of state secrets of high confidentiality to ineligible persons may endanger the sovereignty of the state, territorial integrity and the security of the nation. The release of confidential state secrets may disrupt the administration of the state, national resources and public order; and the disclosure of state secrets of limited confidentiality may disrupt the execution of tasks and functions of the state bodies. However, should every disruption of the execution of tasks and functions of state bodies be seen as a matter of national security? Greater detail should be included in the law to prevent an overly broad interpretation of these provisions.

In the Czech Republic the lowest category of classified information the release of which may be "disadvantageous to the interests of the Czech Republic" is defined as

> the divulgence of classified information to any unauthorized person or misuse of classified information, which can result in the breach of activities of the Armed Forces of the Czech Republic; obstructing, impeding or endangering the vetting or investigation of offences; damage to important economic interests of the Republic, EU or other member states; breach of important commercial or political negotiations of the Czech Republic with a foreign power; or a breach of security or intelligence operations.

The definition of state secrets should be limited only to information that directly relates to the national security of the state and when their unauthorized release would have identifiable and serious consequences.[2] It should also be recommended to limit state secrets to the related activities of national security agencies and not to any public authority in the respective State.

Article IV. Retention Period of State Secrets

According to article 10 of the Indonesian draft law, retention period of state secrets of high confidentiality shall be for a maximum duration of 30 years which is too long even for top secrets. In some countries, the duration of state secrets is tied to the level of classification. The maximum period of time that information can be classified should be limited. The OSCE Representative suggested that "it should be presumed that no information should be classified for more than 15 years, unless compelling reasons can be shown for withholding it."

---

[2] OSCE, The Representative on the Freedom of Media, *Access to Information by the Media in the OSCE Region: Trends and Recommendations. Summary of Preliminary Results of the Survey* (Vienna, 30 April 2007).

Article V. Public Interest

Chapter VI regulates procedures on the protection of state secrets. Government officials with access to classified materials shall be obliged to protect and maintain the confidentiality of state secrets. These state secrets are under their charge and must be protected from any disclosure. However, the public interests test which is accepted in democratic societies should be included to allow the disclosure of information when the public interests outweigh the national security considerations.

Most secret laws contain prohibitions on the classification of certain information for public interest reasons. There are certain international standards on this issue that have been accepted in democratic societies across Europe and elsewhere. For example, according to the Mexican Transparency Law, information may not be classified when the investigation of grave violations of fundamental rights or crimes against humanity is at stake (Article 14).

The Indonesian bill is not clear when it comes to categories of information that should not be classified for reasons of important public interests. According to the OSCE Representative on Freedom of the Media:

> Information relating to violations of the law of human rights, maladministration or administrative errors, threats to public health or the environment, the health of senior elected officials, statistical, social-economic or cultural information, basic scientific information, or that which is merely embarrassing to individuals or organizations should not be classified as a state or official secret.

According to international human rights standards, information relating to human rights violations cannot be classified as state secrets. The information on environmental hazards or personal information about leaders and benefits should not be classified as well. Many countries included respective provisions in their legislation that specify the information that cannot be classified.

Article 8 of the Georgian Law on State Secrets defines the categories of information that cannot be classified as a state secret:

(1) Defining any such information as a state secret that may prejudice or restrict basic human rights or freedoms or may cause harm to health and safety of population shall be prohibited.

(2) Normative acts may not be defined as state secrets except for the acts of the Ministry of Defense, the Ministry of State Security, State Intelligence Department, State Department of Border Guarding and Special Service of State Guarding that regulate their internal activities directly related to state defense and security issues, nor may international agreements and treaties be defined as state secrets.

(3) Maps may not be defined as states secrets, except special military maps.

(4) The following may not be defined as a state secret:

a) information on natural disasters, catastrophes and other extraordinary events which have already occurred or may occur and which threaten the safety of citizens;

b) Information on environmental conditions, health and living standard of the population, including information on medical services and social security, as well as social-demographic data and data on educational and cultural levels of the population;

c) Information on corruption, unlawful actions of the officials and crime statistics;

d) Information on privileges, compensations and benefits provided by the state to the citizens, officials, enterprises, institutions and organizations;

e) Information on the state monetary fund and national gold reserves;

f) Information on health status of the top officials of the state power.

Many countries adopted public interests tests. In some countries (New Zeeland and the UK) a designation of certain information as classified does not prevent its review and possible release under the access to information legislation where the pre-conditions for such a release are defined. In cases of major wrongdoing by a security agency, officials should be able to disclose to the media secret information. In this case, there should not be a threat of prosecution of the media. Thus, even national security information can be released when it is in the public interest to do so.

Journalists shall not be restricted in their activities disproportionally. The right and ability of journalist to release information of public interests should not be curtailed. The state secrecy legislation should not exercise retraining influence on the process of getting and dissemination of information. The government shall not be able to have absolute control upon the contents of news.

The existing wording of the Indonesian law may lead to censorship and can easily be abused, since it gives to the state agencies the absolute power to handle secret information without any meaningful oversight and external control.

Article VI. Whistleblowers' Protection

According to article 29 of the bill, government officials with access to state secrets shall have a duty to protect and maintain the confidentiality of state secrets, and protect state secrets under their charge from being disclosed. However, a civil servant, in the course of his work, may become aware of secret information, whose divulgation or publication corresponds to a strong public interest. In the Indonesian

draft, there is no provision which would explicitly allow access to information of a public interest. There are no protections of whistleblowers who release information of a public interest.

There are certain standards adopted in Europe: the Council of Europe Civil Law Convention on Corruption (CETS No 174) specifies that employees who disclose information about possible corruption should not be subject to sanctions. The OSCE recommended that "whistleblowers who disclose secret information of public interest to the media should not be subject to legal, administrative or employment-related sanctions." The state secrets legislation shall not be used against whistleblowers and journalists. The CoE Parliamentary Assembly also recommended that whistleblowers should be protected: "Look into ways and means of enhancing the protection of whistle-blowers and journalists, who expose corruption, human rights violations, environmental destruction or other abuses of public authority, in all Council of Europe member states."

Unfortunately, the Indonesian Bill enables the public authorities to cover the cases of corruption and maladministration. Thus, a mechanism of whistleblowers' protection should be created by the law that ensures the release of information of strong public interest to the public.

Article VII. Use of Classified Information in Courts

Article 41 of the bill states that court hearings of criminal cases on classified materials shall be closed to the public in order to ensure the protection of such secrets. Such procedures may compromise the principles of a fair trial. In particular, the equality of arms between the prosecution and the defense may be put into question. According to the international guidelines, the defense should be adequately represented in the selection of experts advising the court on the secret nature of relevant information. Such experts should be independent from secret services. The defense shall also be allowed to name experts.

In general, the principle of open and public court hearing should not be compromised. Defendants and their legal representatives should be guaranteed access to all information that is relevant or used in a court or administrative hearings that affects individuals' rights.

Article VIII. Oversight over State Secrets

Some form of parliamentary access to classified information must be guaranteed. Without having such access, the Parliament will not be in a position to implement its functions effectively. It will not be possible to ensure an oversight of military and intelligence services. Investigations into state power abuses and corruption cases

will be limited. The law should provide for an obligation of state bodies to present information to Parliament. Control and approval of the budget should also be a parliamentary prerogative.

Furthermore, it must be ensured that independent bodies outside the intelligence and defence can oversee the activities related to the classification of the information as state secret. The draft fails to guarantee this. Such bodies shall also have the power to declassify the information. In Slovenia, the Information Commissioner was given the power to review information to see if it has been improperly classified. In Indonesia, there is no such independent oversight and control.

According to the Indonesian law, the security and intelligence agencies are less accountable to the elected representatives of the people – the scope of parliamentary oversight and control is reduced. The bill does not give the Parliament the power to exercise control over the legislation and expenditures and does not entail an obligation of the authorities to provide information to the Parliament. There is no parliamentary body which would have unrestricted access to classified information.

According to article 4.1 of the Georgian law on state secrets, the Parliament shall ensure the legislative regulation of protection of information containing a state secret, shall exercise parliamentary control over compliance with the legislation of Georgia on state secrets and with the international agreements, and shall define the authority of those officials in the staff of the Parliament who ensure the protection of state secrets in the Parliament.

The role of Parliament in overseeing the secrecy policy should be expanded.

Moreover, there should be an independent general oversight body which ensures that there is no excessive secrecy. In some countries, there is a Parliamentary Commissioner for Data Protection and Freedom of Information who is entitled to change the classification of state secrets. Such an independent body should not be part of the intelligence, military or security services and should be entitled to receive complaints about improperly classified information and review and order the declassification of information.

The OSCE recommended that "an independent body that is not part of the intelligence, military or security services should have oversight over classified information and ensure that the system is operating properly, receive complaints about improperly classified information and review and order the declassification of information."

Information can be reviewed yearly to ensure that it is still necessary to be classified. When it is no longer necessary, the information should be released. The Advisory Board for State Secret Policy under Chapter V does not constitute an independent mechanism for review and oversight and is not in position to successfully implement these tasks. The Advisory Board for state secret policy consists of

permanent and interim members. Permanent members are the representatives of different state agencies from the executive branch. Interim members may be experts in the field of state secrecy. However, this board is not truly representative since the members of Parliament and the representatives of civil society are not actively and directly involved in its activities.

Furthermore, the competencies of the Board are not specified in the law. The independence of this body may also be put into question, since it will be dealing with the information directly related to the activities of the Ministries and Departments whose heads are sitting on the panel of this board. Thus, this body does not correspond to the principles of democratic accountability, transparency and independence. This mechanism would rather facilitate the culture of secrecy.

Thus, the role of Parliament needs to be enhanced and an independent body should be created to ensure access to information.

Article IX. Classification and Declassification of State Secrets

The law does not specify provisions relating to classifying the information. Article 16 is about the departmental classifications. The departmental head can make a proposal to the President on the classification of certain information as state secrets (article 16). There is a review mechanism. All state secrets are subject to a periodic review which can lead to declassifying the secret information before the end of its retention period. The review is carried out by the head of the state institution. The content of the material and its retention period may be subjected to a periodic review. However, it appears questionable how independent and objective such a review by the departmental heads can be. It is clear that under the existing conditions it will be difficult to bring the cases of corruption and abuse of power to daylight. The power to classify information should not provide to the heads of relevant state administration bodies the power to shield the body from criticism.

It is common practice that each administrative body classifies its own documents. However, this competence should not be unlimited – the activities of administrative bodies shall remain in line with the list of information stipulated in the legal framework (or in an inter-departmental list) and should not constitute an alternative method for classification. Thus, the law should state more specific categories of information to be classified. Review and oversight is essential to make such departmental review system work.

Such classifications must be capable of being annulled by higher authority acting either *proprio motu* or on appeal by an interested citizen. The higher authority must take into account countervailing interests and not simply security concerns.

According to article 20, once the retention period of state secrets ends every person involved therein is neither liable to prosecution nor punishable for any ac-

tion associated with such classified information except in relation to crimes of severe human rights violations and corruption.

The declassification system shall be improved. The information can be changed by reason of changed circumstances (according to the law). It should be possible to declassify information upon citizens' request. There must be a review mechanism that would allow the declassification of information.

There are no provisions that would allow for automatic declassification and release of formerly secret information of public interest. In some eastern European countries, the legislation required that all pre-1990 records be reviewed and those found to be not necessarily kept secret were automatically released. Some of the laws required the review and declassification of all records previously held as state secrets. The OSCE suggested that "all information that was designated as secret by a previous non-democratic government should be declassified and presumptively released unless it can be shown that its release would endanger the national security or be an unwarranted invasion of privacy." Many eastern European countries have adopted laws on the disclosure of secret police files. International organizations recommended that the opening of secret service files in some former communist totalitarian countries to enable the persons affected to examine, upon their request, the files kept on them by the former secret services. The durations of classifications should be reduced. A system should be created that ensures the effective review of classified information and its declassification when it is no longer sensitive.

The law should state the grounds for declassification of classified information. The Georgian law on state secrets is explicit on this point:

Article 17 – The Grounds for Declassification of Secret Information

(1) The following shall constitute the grounds for removal of the secrecy label from the data:
   a) The international obligations undertaken by Georgia with respect to open exchange of such data which previously constituted a state secret;
   b) Change of factual circumstances after which protection of the information previously classified as state secret is no longer needed;
   c) Expiration of the fixed term;
   d) A proposal of the confidence group of the Parliament of Georgia, submitted to the President of Georgia, to remove the secrecy label from the specific information.

The state bodies that classify the information shall be bound to re-examine the classification records annually so as to evaluate the necessity of the classification in each specific case.

The law shall also determine who is entitled to raise the question of declassification of information.

Article X. Access to Personal Data

The law does not regulate the exercise of the *rights of access* to secret files containing personal information. It must always be possible for an individual to challenge before a competent and objective body (judicial or quasi judicial) the holding, by agents of the State, of information on his or her private life or the truth of such information, and, moreover, to obtain correction/deletion of the file where it contains incorrect information or the holding of the information is adjudged unnecessary or disproportionate.

In many countries, the legislation is dealing with the question of access to personal files related to the past abuses of the state agencies (military and security forces). In Australia, for instance, there is an Office of the Privacy Commissioner which is an independent statutory body and whose purpose is to protect and promote privacy in Australia. It was established under the Privacy Act 1988.

In Indonesia, this question does not seem to be part of legislative policy.

One more important issue which is not specified in the law is the transferral of information between state bodies. In this case it is necessary to provide that the original level of classification applies for the agency to which it is transferred and that this agency undertakes to protect the information with the same level of care.

Article XI. Management of State Secrets

The management of state secrets is carried out by the administrator of classified materials. The administrator of state secrets may offer opinions and advice to the head of the state institution in regard to classification. However, the role of the administrators within the system of the protection and maintenance of state secrets is not clear enough. The law does not specify the requirement for their qualifications and other competencies of the administrators. For example, it is not clear if the administrators may also make proposals regarding the declassification and further retention of the classified information.

Article XII. Criminal Proceedings

According to article 35 “any punishable act against state secrecy is an act of crime.” The law does not specify the notion of such punishable acts. Article 37 elaborates that state secrets shall not be used as evidence during court examination except for criminal cases related to disclosure of state secrets. This provision needs further clarification. Does it mean that only the individuals who committed crimes against state secrets can be subjected to such procedures? What about

other grave offences committed by the high ranking officials, what about cases where public interest is at stake? Can classified information be released in the public interest?

In general, the punishments for crimes related to state secrets are too harsh.

The law stipulates that "request for classified material ... shall be submitted in writing by the Chief of the Indonesian Police, Attorney General or the Supreme Court Chief Justice to the head of the state body." The head of the state body has the obligations to provide a response to such request within 30 days. The law does not determine under what circumstances the head of the agency is obliged to disclose the classified information.

Chapter IX contain provisions on criminal punishment of persons who committed offences against state secrets. Thus, this chapter extends to individuals who are in charge of state secrets' protections and other individuals who possess the classified information and are obliged to give this information to the competent authorities.

Conclusions and Recommendations

- The bill should limit the scope of state secrecy.
- There should be more specific provisions regarding the categories of information to be classified as state secrets.
- The Indonesian law does not provide guidance as to what is a gross infringement of Indonesian security (it is up to the courts to interpret the letter of the law). Thus, the bill should include more specific provisions in this regard.
- The application of the law should be reduced only to information the release of which would harm national security.
- The duration of classifications should be reduced. The law should regulate the issue of extensions of classifications. Any such extension should be separately justified.
- A system should be put in place to ensure the effective review of classified information and its declassification when it is no longer sensitive. An independent body should be created to enforce freedom of information legislation with the power to review state secrets decisions to ensure access to information.
- There should be certain information that should be automatically declassified. This information may be related to or classified by the previous dictatorships in Indonesia. The information must be determined by the law

which cannot be designated as state secrets for reasons of public interest in disclosing such information under any circumstances.

- The categories of information that cannot be classified as a state secret should be expanded. This should include information on all violations of human rights standards, violations of law, maladministration and other important categories already emphasized above.
- Whistle-blowing protections should be included to ensure the release of information of strong interest to the public. The interests of journalists must be guaranteed.
- Limits on access to secret information should be proportional. Citizens should be able to have access to elected officials, judges.
- The principles of a fair trial should not be compromised for reasons of national security.
- Defendants and their legal representatives should be guaranteed access to all information that is relevant in a court or administrative proceedings that affects a person's civil, political or socio-economic rights.
- The principle of open and public court hearings should be maintained.
- The role of Parliament in overseeing the activities related to the classification of information should be strengthened. The parliamentary committees may play a crucial role in this respect.

Indonesian Draft "Secrecy Law"

Michael Noone

Introduction

"Transparency" and "accountability" are important characteristics of any state which claims to be democratic. Citizens must see how the business of government is being carried on in order to hold governments, state entities and, in some cases, state agents responsible for their actions and expenditures.[1]

Therefore, any law which seeks to limit disclosure should be treated as an exception to the premise that, unless otherwise required by statute (i.e., a law passed by the legislature), matters of official record shall, in accord with published rules, be available to the public. Article 19 of the International Covenant on Civil and Political Rights provides:

> Everyone has the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas, regardless of frontiers, either orally, in writing, or in print, in the form of art, or through any other media of his choice. (paragraph 2)
>
> The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> a) For respect of the rights or reputations of others;
>
> b) For the protection of national security or of public order, or of public health or morals.

Indonesia ratified and acceded to the Covenant in 2006. I understand that in April 2008 Indonesia passed a Freedom of Information Act (FOI) which will be implemented in 2010. A press report, filed shortly after passage of the Act, stated:

---

[1] David Greenwood and Sander Huisman's "Introduction and Methodology," in *Transparency and Accountability of Police Forces, Security Services and Intelligence Agencies*, DCAF & CESS (Sofia: GCMA-Bulgaria, 2004).

> The FOI law calls for creating independent public information commissions at provincial or even district levels, if deemed necessary. Its members will be nominated by the public and approved by legislators. Its core function is to settle disputes that may arise over the use or failure to obtain information from a bureaucratic institution.

However, the law says that commissioners cannot help mediate in cases of:

- State intelligence
- Information pertaining to national defense, security, and resources
- Information pertaining to economic, foreign, and private interests
- Memos exchanged among private companies.[2]

It is within this context that I will compare and contrast the U.S. approach with that of Indonesia.

Relevant U.S. Laws

The Freedom of Information Act (FOIA) was signed into law by President Lyndon Johnson on July 4, 1966 and went into effect on July 4, 1967. Previously government agencies were guided by section 3 of the Administrative Procedure Act of 1946 which provided that "matters of official record shall in accordance with public rule be made available to persons properly and directly concerned except information held confidential for good cause shown." This provision, which could be traced to the original (1789) statute establishing the Federal government's Executive Branch also excluded from public scrutiny any function of the United States requiring secrecy "in the public interest" and "any matter relating solely to the internal management of an agency." Congress concluded that agencies had abused the discretion. In their introduction to the joint report "Freedom of Information Act and Amendments of 1974 (P.L. 93-502)" the Senate and House of Representatives Committees responsible for the legislation summarized the changes:

> The Freedom of Information Act replaced [the previous] general language relating to secrecy, indicating that Congress, in enacting the act, has adopted a policy that "any person" should have clear access to identifiable agency records without having to state a reason for wanting the information and that the burden of proving withholding to be necessary is placed on the Federal agency.

---

[2] Niki Swartz, "Indonesia Passes New FOI Law," *Information Management Journal* 1 (July/August 2008), www.entrepreneur.com/tradejournals/article/184324900.html.

Withholding of information by the government under the act is permissive, not mandatory, and must be justified on the basis of one of the specific nine exemptions permitted in the act. These relate to matters that are –

1. Specifically required by Executive order to be kept secret in the interest of national defense or foreign policy;
2. Related solely to the internal personnel rules and practices of an agency;
3. Specifically exempted from disclosure by statute;
4. Trade secrets and commercial or financial information obtained from a person and privileged or confidential;
5. Inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
6. Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
7. Investigatory files complied for law enforcement purposes except to the extent available by law to a party other than an agency;
8. Contained in or related to examination, operating, or condition report prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
9. Geological and geophysical information and data, including maps, concerning wells.

The act makes it clear in section 552(c) that the exemptions have absolutely no effect upon congressional access to information:

> This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in the section. This section is not authority to withhold information from Congress.

If this statute were to be used as an exemplar for other countries, they would have to accept its premises:

- Everything that is a public record may be disclosed (by someone having the authority to do so)
- Some public records may (but need not be) exempt from disclosure (by whoever is given the authority to claim a specified exemption)
- Many of the exemptions are based on Common Law rules regarding the admissibility of evidence in law suits, thus the "terms privileged" in exemption 4 and "clearly unwarranted invasion of personal privacy" in exemption

6; and notions of reciprocity, "not available ... to others [not] in litigation" (exemption 5); "investigatory files ... available by law..." (exemption 7) would have to be revised to conform with other legal systems' rules

- Neither the Legislative nor the Judicial Branch is bound by these provisions
- Some degree of judicial involvement in the resolution of disputes is assumed, e.g., a court may be called on to decide whether disclosure would be "a clearly unwarranted invasion of privacy" or whether Common Law rules regarding the admissibility of evidence apply to the particular information sought. However, under the U.S. system, the President, not the courts, has the authority to decide whether certain information is "to be kept secret in the interest of national defense or foreign policy." Other national legal systems may not provide for judicial intervention when a government action, e.g., refusal to disclose information, is challenged.

The fundamental U.S. Secrecy law is not a statute, passed by Congress, but an Executive Order, issued by the President exercising his constitutional obligations to "take care that the laws are faithfully executed," to command the army and the navy, and to serve "as the sole organ of the government in its external relations" (U.S. Supreme Court in the *Curtis Wright* case, 299 U.S. 304 (1936)). Executive Orders are issued to direct the bureaucracy and are granted great deference by the courts if the President's judgment is challenged.

Executive Order 12958 "Classified National Security Information" was issued by President Clinton in 1995 and amended (Executive Order 13292) by President George W. Bush in 2003. Although President Obama will probably direct changes in content, the essential structure of the Order offers a framework which can be compared with the Indonesian proposal.

1. Who can classify information, the authority to delegate, classification by levels of access (Confidential, Secret, Top Secret) and what information can be classified, which is subject to the following proviso: "Information shall not be considered for classification unless it concerns: military plans, weapons systems or operations; foreign government information; intelligence activities, intelligence sources or methods, or cryptology; foreign relations or foreign activities, including confidential sources; scientific, technological, or economic matters relating to national security, which includes defense against transnational terrorism; government programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to na-

tional security, which includes defense against transnational terrorism; or weapons of mass destruction"; the duration of classification; the marking of classified documents. Of particular interest is the provision regarding Classification prohibitions and limitations: "In no case shall information be classified in order to conceal violations of law, inefficiency, or administrative error; prevent embarrassment to a person, organization, or agency; restrain competition, or prevent or delay the release of information that does not require protection in the interest of national security"; provisions for reclassification after declassification; provisions for classifying hitherto unclassified information if it is sought under the Freedom of Information Act.

2. "Derivative Classification" which permits persons who do not have classification authority to reproduce, extract or summarize classified material to carry forward the original classification (and declassification date) to the newly originated documents and provisions requiring that guides be published to establish standards for derivative classification.
3. Declassification and Down Grading of classified information.
4. Provisions for Safeguarding classified information.
5. Provisions for implementing the Order at the agency level and exercising internal (i.e., Executive Branch) oversight of agency actions under the Order.
6. General Provisions, including a list of definitions.

The Proposed Indonesian Secrecy Law

I will not comment on the legislative format since that it is a matter of national style. My comments will focus on the substance of the legislation.

1. Preamble: No comment. I don't know whether broad statements of principle have any legal efficacy. The title of the statute doesn't conform with the ideals of the ICCPR. I suggest "Law for the Protection of National Security."
2. Chapter 1, article 1: – the term "state secret," as defined, could encompass anything the President, or his designees, decide would be disruptive. I suggest the provision be rewritten to serve as an exception to the Freedom of Public Information law. The inclusion of "non legal entities" in paragraph 7 is unusual. And the definition of "creator" in para. 9 is far too broad. In order to achieve transparency and accountability the best practice would be to designate a person or office within the state body. The same observation applies to the term "authorized institution" in para. 14. Para. 12 indicates that requests would be made under the secrecy law. They should be submitted under the Public Information law.

3. Chapter 1, Article 2. If this is intended to have some legal efficacy it is far too broad. Best practice suggests that classification should be an exception to the free flow of information and should be done only by designated individuals and offices. Then, see the nine exemptions in the US FOIA.
4. Article 3: an unusual (to my eyes) categorization. I don't know why it is necessary.
5. Article 4: I don't know what the "separate law" is/would be.
6. Article 5: Is "confidentiality" synonymous with "secrecy?"
7. Article 6.a (1) and (2) information related to state defense – refer to the U.S. approach "military plans, weapons systems or operations." In the Common law the doctrine *inclusio unius est exclusio alterius* means that an item which is not included in a comprehensive list isn't covered. Perhaps the fact that this is a statute and the legislature desires specificity justifies the approach. The same observation applies to paras 3 (intelligence), 4 (cryptology) and 5 (foreign relations). With regard to para. 6, compare US Treasury Order 105-19 (available at www.ustreas.gov/regs/to105-19.htm) which designates offices authorized to classify, not information which may be classified. Article 6.b. is apparently intended to authorize making secret anything else that hasn't been listed previously.
8. Article 7 and 8. Compare the criteria in U.S. Executive Order 13292 sec 1.2: Top Secret: disclosure would cause "exceptionally grave damage to the national security that the original classification authority is able to identify or describe;" Secret "…serious damage" etc…; "confidential ... damage etc..."
9. Article 9: I don't understand the purpose of this provision. It may have been mistranslated because Article 28(3) gives the impression that it is a classification – although the character of the information protected is not defined. However the Criminal Provisions (Articles 44–46) apply only to two categories of secrecy.
10. Article 10. Para. (1) and (2) are adequate since they establish a maximum duration. Best practice would be to provide for periodic review and possible earlier declassification. Para. 3: I don't understand the purpose of this provision. If, for example, Highly confidential information has been compromised by one person to one recipient, why must it be declassified within five years rather than thirty? See Article 19.
11. Articles 11–13: similar to U.S. practice but, with regard to Articles 13(2), 14 and 15, I don't understand the term "state body." Does it relate to the Legislature? I'm not aware of any nation which permits its legislature to formally

designate material as secret. Typically, the Legislature's internal rules permit, for example, confidentiality and disclosure in the Common Law tradition and would call for punishment by contempt hearings or by reference to the judiciary.

12. Article 16: similar to the US practice "damage which the original classification authority can identify or describe."
13. Article 17, 18, 19 and 20: good practice – no comment.
14. Articles 21–25: unremarkable. The U.S. has established a different procedure which relies on the President's National Security Advisor and the National Archivist. Perhaps the Indonesian equivalent would be the interim appointee referred to in Article 22(3). Someone expert in record retention should be member of the Board. In this regard see Article 30.
15. Articles 26–29: no comment.
16. Articles 30–33. I am not aware of any similar official designation in other national systems. While the goal is understandable, several questions arise. Does Indonesia have someone responsible for the National Records of the Executive? What would this person's relation be to whom I would refer to as the Archivist? Subordinate? Superior? Equal? The State Intelligence Agency grants Security Clearances (Article 28). Why does the Encryption Agency certify the Administrator's qualifications?
17. Articles 42–49. I have no comment regarding the proposed penalties (Articles 44-46). And my comments regarding the proposed procedure are not informed by any particular knowledge of Indonesian Criminal Procedure. I have the following general comments: Article 42 makes the law applicable to persons who commit a crime within Indonesia; and Article 43 makes law applicable to crimes outside Indonesia. I don't understand why two Articles are needed instead of a statement of general jurisdiction. I don't know how Indonesian law defines "intent" (Articles 44 and 45). How would that be established? Intent to do the act? Or intent in the sense of knowing the consequences? What are "activities associated with state secrecy." Does that mean they have been classified? That provision endangers free press.
18. Articles 36–41 should be examined by someone familiar with Indonesian Criminal Justice standards as well as International Human Rights Standards. Will the accused person be granted access to all the evidence on which the charge is based (see Article 38). How can he challenge the explanatory letter? Can the defendant submit a request for classified material in order to

defend himself (Article 39)? What provisions are made for qualifying the accused's lawyer to examine the material?

Philipp Fluri, ed., *The Indonesian Draft State Secrecy Law. Four International Perspectives*, DCAF Regional Programmes Series # 3 (Geneva: Geneva Centre for the Democratic Control of Armed Forces, May 2010).

DCAF Regional Programmes Series no. 3

Original version: English, Geneva, 2010

Geneva Centre for the Democratic Control of Armed Forces
< www.dcaf.ch>
P.O.Box 1360, CH-1211 Geneva 1, Switzerland

Cover Design: Hristo Bliznashki

Format: 6.25 x 9

ISBN 978-92-9222-141-6

The Geneva Centre for the Democratic Control of Armed Forces (DCAF)

DCAF was established in 2000 by the Swiss government. DCAF is an international foundation with 53 member states and the Canton of Geneva. DCAF's main divisions are Research, Operations and Special Programmes. The staff numbers over 70 employees from more than 30 countries. DCAF's head office is located in Geneva, Switzerland. The Centre also has permanent offices in Brussels, Ljubljana, Ramallah and Beirut.

The Geneva Centre for the Democratic Control of Armed Forces is one of the world's leading institutions in the areas of security sector reform and security sector governance. DCAF provides in-country advisory support and practical assistance programmes, develops and promotes appropriate democratic norms at the international and national levels, advocates good practices and conducts policy-related research to make recommendations to ensure effective democratic governance of the security sector.

DCAF's partners include governments, parliaments, civil society, international organisations and the range of security sector actors such as police, judiciary, intelligence agencies, border security services and the military.

www.dcaf.ch

ISBN 978-92-9222-141-6

DCAF Regional Programmes Series no. 3