MEMORANDUM

on

Jordan's Protection of State Secrets & Documents Provisional Law No. (50)

London
December 2005

ARTICLE 19 · 6-8 Amwell Street · London EC1R 1UQ · United Kingdom
Tel +44 20 7278 9292 · Fax +44 20 7278 7660 · info@article19.org · http://www.article19.org

TABLE OF CONTENTS

1. Introduction

This Memorandum provides an analysis of the Protection of State Secrets & Documents Provisional Law No. (50) for the year 1971 (the 'Law') for the Hashemite Kingdom of Jordan. The Law enables officials to protect broad categories of information as state secrets and imposes strict liability offences with severe criminal sanctions on any person who violates its provisions. The Law raises concerns in regard to overly broad definitions of key terms as well as the absence of protections necessary to ensure the right to freedom of information. ARTICLE 19 notes that secrecy laws such as the present Law should define national security precisely and indicate clearly the criteria which should be used in determining classified information, so as to prevent abuse of the label 'secret' to prevent disclosure of information in the public interest.

The Jordanian government, at the highest level, has committed itself over several years to a process of modernisation and democratisation and has also voluntarily entered into treaty agreements with other States according to which it has undertaken to respect human rights, including freedom of expression and information. Welcoming these reform initiatives, ARTICLE 19 has been active in Jordan for several years, providing expertise on a range of other legislative proposals.[1] The purpose of this Memorandum is to identify pressing matters of legal reform which violate Jordan's obligations under international law.

This Memorandum addresses the freedom of information issues within the Law. ARTICLE 19's analysis and comments are made within the framework of the applicable international standards, with particular reference to Jordan's treaty obligations under the *International Covenant on Civil and Political Rights* (ICCPR). These standards are outlined in Section Two of this Memorandum and Section Three sets forth our analysis and proposed amendments to bring the Law more fully in line with these standards.

The overbreadth and vagueness of the provisions of the Law pose a serious threat to the right to freedom of information as guaranteed under international law. While the Law is ostensibly directed at protecting highly sensitive political and military material, the classification scheme is exceptionally broad allowing for almost any information to be excluded from public view, facilitating a culture of government secrecy and lack of accountability and repressing the media's role as a public 'watchdog'. We are particularly concerned by the wide ambit of who may classify information – the Law allows any private or public person connected with the information to do so – and the complete lack of accountability for the decision to classify information including the absence of a review mechanism to de-classify information after the lapse of time. Once classified, the information remains protected indefinitely under the Law. It is fundamental to the principles of freedom of information that the time-sensitivity of the information is accounted for in assessing whether the information poses a risk of substantial harm to national security. Finally, it is unsustainable to couple severe criminal sanctions with strict liability offences, whose application is broad and undefined. These provisions require further consideration and redrafting to reflect their proposed purpose.

[1] See, for example, Memorandum on Jordan's proposed 1998 Press and Publications Law, July 1998; Memorandum on the Provisional Audiovisual Media Law, February 2005.

2. International Standards

2.1 Freedom of Expression and Information

Secrecy laws impact both on the right of individuals to express themselves – for example, by placing restrictions on what may be published in the media – and on the right of everyone to access information held by a public body.

Both the right to freedom of expression and the right to access information are well-established in international law – the latter as part of the former. Freedom of expression has been guaranteed through Article 19 of the *Universal Declaration on Human Rights* (UDHR), adopted in 1948,[2] and through Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR), adopted in 1966.[3] Jordan also signed the *Arab Charter on Human Rights* (ACHR)[4], but never ratified it. The ACHR specifically enshrines a guarantee of freedom of expression.

The right to access information held by public bodies is a fundamental human right recognised in international law as part of Article 19 of the UDHR and ICCPR, which guarantee a right of all to *seek and receive* information. It is crucial as a right in its own regard as well as central to the functioning of democracy and the enforcement of other rights. Without freedom of information, State authorities can control the flow of information, 'hiding' material that is damaging to the government and selectively releasing 'good news'. In such a climate, corruption thrives and human rights violations can remain unchecked. If the information is politically sensitive material relating to national security it may be exempted from disclosure but only if a number of safeguards are first established.

For this reason, international bodies such as the United Nations Special Rapporteur on Freedom of Opinion and Expression[5] have repeatedly called on all States to adopt and implement freedom of information legislation.[6] State secrets and sensitive information must be subject to the operation of such legislation, and other Laws must be consistent with it. We also draw attention to the Declaration of the Special Rapporteurs on freedom of expression outlining the relevant principles applying to freedom of information and secrecy legislation, in which they stress that secrecy laws must be narrowly drafted and be compatible with the right to access information.[7]

---

[2] *UN General Assembly Resolution 217A (III)*, adopted 10 December 1948.
[3] *UN General Assembly Resolution 2200A (XXI),* adopted 16 December 1966, in force 23 March 1976. Jordan ratified the ICCPR in 1975.
[4] Adopted on 15 September 1994. See Article 26 of the ACHR.
[5] The Office of the Special Rapporteur on of Opinion and Expression was established by the UN Commission on Human Rights, the most authoritative UN human rights body, in 1993: Resolution 1993/45, 5 March 1993.
[6] See, for example, the Concluding Observations of the Human Rights Committee in relation to Trinidad and Tobago, UN Doc. No. CCPR/CO/70/TTO/Add.1, 15 January 2001. 14. The comments of the UN Special Rapporteur on freedom of Opinion and Expression are discussed at length below.
[7] Available at http://www.cidh.org/Relatoria/showarticle.asp?artID=319&lID=1. The Special Rapporteurs are the UN Special Rapporteur on Freedom of Opinion and Expression; the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression.
[12] For judicial opinions on human rights guarantees in customary international law, see *Barcelona Traction, Light and Power Company Limited Case* (Belgium v. Spain) (Second Phase), ICJ Rep. 1970 3 (International Court of Justice); *Namibia Opinion*, ICJ Rep. 1971 16, Separate Opinion, Judge Ammoun (International Court of Justice); *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (US Circuit Court of Appeals, 2nd Circuit). For an academic critique, see M.S. McDougal, H.D. Lasswell and L.C. Chen, *Human Rights and World Public*

Article 19 of the UDHR, which was adopted as a United Nations General Assembly resolution, states:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

While the UDHR is not directly binding on States, parts of it, including Article 19, are widely regarded as having acquired legal force as customary international law.[12] In addition, the ICCPR is a formally binding legal treaty ratified by 154 States;[13] it ensures the right to freedom of expression and information in terms similar to the UDHR. Both Article 19 of the UDHR and Article 19 of the ICCPR have been interpreted as imposing an obligation on States to implement measures to enable access to information held by public bodies.

The content of these treaty obligations have been developed by the UN Special Rapporteur on Freedom of Opinion and Expression and these measures have been recognised and supported by the UN Commission on Human Rights as critical to the proper enforcement of States' treaty obligations under Article 19.[14] In 1995, the UN Special Rapporteur on Freedom of Opinion and Expression stated:

Order, (Yale University Press: 1980), pp. 273-74, 325-27. See also United Nations General Assembly Resolution 59 (1), 1946.

[13] As of 27 April 2005..

[14] Resolution 1997/27, 11 April 1997. 12(d).

> The Special Rapporteur, therefore, underscores once again that the tendency of many Governments to withhold information from the people at large … is to be strongly checked.[15]

In November 1999, the UN Special Rapporteur was joined in his call by his regional counterparts, bringing together all three special mandates on freedom of expression – the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Representative on Freedom of the Media of the Organisation for Security and Cooperation in Europe and the Special Rapporteur on Freedom of Expression of the Organisation of American States. They adopted a Joint Declaration which included the following statement:

> Implicit in freedom of expression is the public's right to open access to information and to know what governments are doing on their behalf, without which truth would languish and people's participation in government would remain fragmented.[16]

A rapidly growing number of States have now recognised the importance of freedom of information and have implemented laws giving effect to the right. In the last fifteen years, a range of countries including India, Israel, Japan, Mexico, South Africa, South Korea, Sri Lanka, Thailand, Trinidad and Tobago, Guatemala, the United Kingdom and most East and Central European States have adopted freedom of information laws. In doing so, they join a large number of other countries that have enacted such laws some time ago, including Sweden, the United States, Finland, the Netherlands, Australia and Canada.

2.2 Restrictions to Freedom of Expression and Information

One of the key issues in freedom of expression and information is defining when a public body can refuse to disclose information, or when the exercise of freedom of expression may be restricted. Under international law, freedom of information may be subject to restrictions, where those restrictions meet the requirements stipulated in Article 19(3) of the ICCPR:

> The exercise of the rights [to freedom of expression and information] 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 (ordre public), or of public health or morals.

Any restriction on freedom of expression and information must meet a strict three-part test, as recognised by the UN Human Rights Committee. This test requires that any restriction must a) be provided by law, b) be for the purpose of safeguarding one of the legitimate interests listed, and c) be necessary to achieve this goal.

The first condition, that any restrictions should be 'provided by law,' is not satisfied merely by setting out the restriction in domestic law. Legislation must itself be in accordance with human rights principles set out in the ICCPR.[17] The European Court of Human Rights, in

[15] Report of the Special Rapporteur, 4 February 1997, *Promotion and protection of the right to freedom of opinion and expression*, UN Doc. E/CN.4/1997/31.
[16] 26 November 1999.
[17] *Faurisson v. France*, Decision of 8 November 1996, Communication No. 550/1993 (UN Human Rights

its jurisprudence on the similarly worded ECHR provisions on freedom of expression, has developed two fundamental requirements:

> First, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[18]

The second condition requires that legislative measures restricting free expression must truly pursue one of the aims listed in Article 19(3) of the ICCPR, namely the protection of the rights or reputations of others or of national security, public order (*ordre public*) or public health or morals.

The third condition means that even measures which seek to protect a legitimate interest must meet the requisite standard established by the term "necessary." This is a very strict test:

> [The adjective 'necessary'] is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable". [It] implies the existence of a "pressing social need."[19]

Furthermore, any restriction must restrict freedom of expression as little as possible.[20] The measures adopted must be carefully designed to achieve the objective in question, and they should not be arbitrary, unfair or based on irrational considerations.[21] Vague or broadly defined restrictions, even if they satisfy the "provided by law" criterion, are unacceptable because they go beyond what is strictly required to protect the legitimate interest.

Both the UN Human Rights Committee and the European Court of Human Rights have on several occasions had to deal with cases in which States have sought to justify restrictions on freedom of expression or other human rights by reference to national security considerations.

The UN Human Rights Committee, for example, has made it clear that the onus is on the State seeking to justify a restriction based on grounds of national security by reference to a specific threat. In the case of *Jong-Kyu v. Republic of Korea*,[22] for example, the government had claimed that a national strike in any country would pose a national security and public order. The Committee held that this failed to pass the necessity part of the test.

In a similar vein, the European Court has warned that laws that restrict freedom of expression on national security grounds must lay down clear and precise definitions, so as to safeguard against abuse.[23] The Court has issued repeated warnings against excessive use

---

Committee).

[18] *Sunday Times v. the United Kingdom*, Judgment of 26 April 1979, Application No. 6538/74, para. 49 (European Court of Human Rights).

[19] *Ibid.*, para. 59.

[20] *Handyside v. the United Kingdom*, Judgment of 7 December 1976, Application No. 5493/72, para. 49 (European Court of Human Rights).

[21] See *R. v. Oakes* (1986), 26 DLR (4th) 200, at 227-8, (Canadian Supreme Court).

[22] Communication No. 518/1992, views adopted July 1995.

[23] See, for example, *Klass v. FRG*, Application No. 5029/71, 6 September 1978.

of national security laws, in many cases finding violations of fundamental human rights. In a recent case concerning Romania, involving data that had been gathered on the applicant by the security services, the Court noted that it had "doubts as to the relevance to national security of the information."[24] It went on to find a violation of the applicant's rights.

The Court has also warned against the use of national security laws even in situations of armed internal conflict. While stressing that it would not condone the use of the media as a mouthpiece for advocates of violence, it has said that States "cannot, with reference to the protection of territorial integrity or national security or the prevention of crime or disorder, restrict the right of the public to be informed by bringing the weight of the criminal law to bear on the media."[25]

2.2.1 Specific requirements for restrictions relating to freedom of information

Further to the standard three-part test for restrictions on freedom of expression, there is specific guidance on when a public body is under an obligation to disclose information. These criteria reflect the general requirements of the restrictions test but provide a more detailed test for issues pertaining to freedom of information.

Accordingly, in line with Article 19(3) of the ICCPR, a public body must disclose any information which it holds and is asked for, unless:

1. The information concerns a legitimate protected interest listed in the law;
2. Disclosure threatens substantial harm to that interest; and
3. The harm to the protected interest is greater than the public interest in having the information.[26]

1. Legitimate Protected Interest

Freedom of information laws must contain an *exhaustive* list of all legitimate interests on which a refusal of disclosure is based. This list should be limited to matters such as law enforcement, the protection of personal information, national security, commercial and other confidentiality, public or individual safety, and protecting the effectiveness and integrity of government decision-making processes.[27]

Exceptions should be narrowly drawn to avoid capturing information the disclosure of which would not harm the legitimate interest. Furthermore, they should be based on the content, rather than the type of document sought. To meet this standard, exceptions should, where relevant, be time-limited. For example, the justification for classifying information on the basis of national security may well disappear after a specific national security threat subsides.

2. Substantial Harm

Once it has been established that the information falls within the scope of a legitimate aim listed in the legislation, it must be established that disclosure of the information would cause substantial harm to that legitimate aim.

[24] *Rotaru v. Romania*, 4 May 2000, Application No. 28341/95, para. 53.
[25] *Erdogdu and Ince v. Turkey*, 8 July 1999, Application Nos. 25067/94 and 25068/94, para. 54.
[26] See ARTICLE 19's *The Public's Right to Know*, at Principle 4.
[27] *Ibid.*

In some cases, disclosure may benefit as well as harm that aim.

3. Harm outweighs public interest benefit in disclosure

The third part of the test requires the public body to consider whether, even if disclosure of information causes serious harm to a protected interest, there is nevertheless a wider public interest in disclosure. For instance, in relation to national security, disclosure of information exposing instances of bribery may concurrently undermine defence interests and expose corrupt buying practices. The latter, however, may lead to eradicating corruption and therefore strengthen national security in the long-term. In such cases, information should be disclosed notwithstanding that it may cause harm in the short term.

Cumulatively, the three-part test is designed to guarantee that information is only withheld when it is in the overall public interest. If applied properly, this test would rule out all blanket exclusions and class exceptions as well as any provisions whose real aim is to protect the government from harassment, to prevent the exposure of wrongdoing, to avoid the concealment information from the public or to preclude entrenching a particular ideology.

2.2.2 Guidance on restrictions to freedom of expression and information – national security

Finally, a specific set of minimum principles related to restrictions on national security grounds has also been set out in the *Johannesburg Principles on National Security, Freedom of Expression and Access to Information* ("Johannesburg Principles"), adopted in October 1995 by a group of experts in international law and human rights convened by ARTICLE 19 and the Centre for Applied Legal Studies of the University of the Witwatersrand. The Johannesburg Principles have since been endorsed by the UN Special Rapporteur on Freedom of Opinion and Expression and are used as a reference tool by the UN Commission on Human Rights.[28] They recognise that the right to seek, receive and impart information may, at times, be restricted on specific grounds, including the protection of national security. However, national security cannot be a catch-all for limiting access to information. The following principles are of particular relevance:

> **Principle 2: Legitimate National Security Interest**
>
> (a) A restriction sought to be justified on the ground of national security is not legitimate 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 6: Expression That May Threaten National Security**

[28] See UN Doc. Nos. E/CN.4/RES/2003/42, E/CN.4/RES/2002/48, /CN.4/RES/2001/47, E/CN.4/RES/2000/38, E/CN.4/RES/1999/36, E/CN.4/RES/1998/42, E/CN.4/RES/1997/27 and E/CN.4/RES/1996/53. For example, in his 2003 and 2004 reports to the UN Commission on Human Rights: UN Doc. Nos. E/CN.4/2004/62 and E/CN.4/2003/67.

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 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.

We refer to these Principles below where relevant to the provisions of the Law.

3. Analysis of the Law

3.1 Overview

The Law sets out categories of information that may be protected as state secrets and imposes criminal sanctions on persons who violate the Law. Article 2 defines "department," "officer," and "protected secrets and document." Articles 3, 6 and 8 set out and define three classification levels - 'strictly confidential,' 'confidential' and 'restricted' respectively. Articles 4, 5, 7 and 9 describe the manner in which any officer in possession of such information should envelop, dispatch and protect classified information. Article 10 defines all official documents that do not satisfy the requirements set forth in Articles 3, 6 and 8 as "ordinary" and not subject to disclosure to "non-concerned persons". Articles 11, 12, 13 and 16 create duties for any persons who have access to official State information and establish criminal sanctions for certain offences. Articles 14 and 15 set down the criminal sanctions for persons who steal or attempt to steal any protected information. Article 17 repeals articles of Penal Law No. (16) for the year 1960 and of the Military Penal Law No. (43) for the year 1952. Article 18 grants the Council of Ministers, with the King's consent, the power to issue regulations for the implementation of the Law. Article 19 charges the Prime Minister and Ministers with the implementation of the provisions of the Law. Articles 1 and 17 are absent from the analysis below as they do not pose issues relating to freedom of information.

3.2 Scope of the Law

The Law applies to both public and private entities and a wide range of information. Article 2 defines department as "any ministry, department, governmental or private institution that maintains, by the nature of its work or production secrets, official documents or information, whose disclosure form a threat to the internal or external security of the State." Article 2 also defines "protected secrets and document" as "any oral information, or a document which is written, typed, stenographed or printed on waxed or duplication paper,

recording tapes, photographs, films, layouts, drawings, maps or similar and classified document according to the provisions of this law".

The Law defines an officer as "any Minister, Director, Chief, commander or employee whose nature of work requires the maintenance or access to official documents or general information whose disclosure form a threat to the internal or external security of the State." Article 11 provides that the "strictly confidential protected, confidential, restricted and ordinary documents are considered under the custody of the person responsible for them."

Analysis

The Law considers that private entities and individuals may possess State secrets. We consider that the appropriate scope of the Law – that is, restricting access to information in which there is a substantial risk of harm to national harm which outweighs the public interest in its disclosure – is such that *no* private institutions would legitimately possess such information. We cannot foresee any situation where the government would outsource sensitive national security information to an external private institution. Accordingly, the scope of the definition of Department should be drafted considerably more narrowly than currently worded in Article 2 removing, at a minimum, private institutions.

Also, the phrase "secrets, official documents or information" in the current definition of "department" is particularly problematic. The scope of the information held by the "department" must be more clearly circumscribed than this. At the least, the definition should be limited to information which falls within the definition of "protected secrets and document" and thus defined within the Law.

Article 2 also fails to adequately define the boundaries of "protected secrets and document" allowing an unlimited range of information to fall within the definition. While we note this may be in part due to the process of translation, the scope of the definition of "protected secrets and document" in Article 2 is very unclear. Is it intended that the definition is limited to documents classified under the Law, or is intended to be a non-exclusive definition? We are concerned that a very broad range of material can be encompassed under the current drafting of "protected secrets and documents". As noted above, secrecy laws such as the present Law should define national security precisely and indicate clearly the criteria which should be used in determining classified information, so as to prevent abuse of the label 'secret' to prevent disclosure of information in the public interest. An expansive, broadly drafted definition of "protected secrets and documents" is inconsistent with the international standards which govern access to information and potentially encompasses a significant amount of information which is not necessary to protect national security.

Also, while the Law purports to protect only classified documents, the scope of the classification definitions are so broad that potentially any information could be included in these categories. Again, this a cause for serious concern. The classification system, in conjunction with the definition of "protected secrets and document", is critical in defining the proper scope of secrecy legislation and is in need of substantial review.

There are serious issues relating to who has the authority to classify information, the lack of a review mechanism for the decision to qualify information, and the definition of "ordinary documents" which seeks to place all official documents beyond disclosure to "non-concerned persons". Accordingly the scope of the Law is very broad indeed, far beyond the

intended purpose of the Law. We urge reconsideration of the classification of all official documents as "ordinary documents" which are excluded from public view. This is a category of classification which does not have any justification. We outline our comments and reccomendations on Article 10 below at Section 3.3.1. The related issues regarding which persons are authorised to classify information and the need for a review mechanism are addressed at Sections 3.3 and 3.5 below.

Recommendation

- The definitions of "department" and "protected secrets and document" should be amended as outlined above.

3.3 Restrictions on access - classification of information

3.3.1 Categories of classification

Article 3, which protects the most sensitive information, provides that protected secrets or documents shall be classified as 'strictly confidential' if it contains:

a. Any information the disclose of its contents to persons whose nature of work does not require access thereto, retaining or possessing thereof would lead to the occurrence of serious damages to the internal or external security of the State or (provide) great benefit to any other State which would form or may form a threat to the Hashemite Kingdom of Jordan.
b. Plans and details of military operations, public security or general intelligence measures or any plan of general relation to military operations or internal security measures, whether economic, production, supply, construction or transportation.
c. Highly important and serious political documents relating to international relations, agreements, conventions and all relating discussions and studies therewith.
d. Information and documents relating to the methods of military intelligence, general intelligence, counter intelligence, espionage resistance or any information affecting the sources of military intelligence and general intelligence or persons working therein.
e. Very important information relating to arms, ammunition or any other source of defence force whose disclosure forms a threat to the internal or external security of the State.

Article 6 classifies any secrets or protected documents as 'confidential' containing:

a. Any important information, the disclosure of the context thereof to persons whose nature of work does not require having access thereto, would lead to a threat to the security of the State, cause damage to its interests or be of great benefit to any foreign State or any other party.
b. Any information on the sites for piling the defence or economic materials or vital institutions relating to sources of power whenever it touches upon the security of the State.
c. Any information on the movement of the armed forces or public security.
d. Any information on the weapons and forces of the sister Arabic States.

Article 8 classifies information as 'restricted' if it contains:

a. Any information whose disclosure to persons authorized to have access would lead to the detriment of the interests of the State, form an embarrassment to it, cause administrative or economic difficulties for the country or be of benefit to a foreign State or any other party which may reflect a detriment on the State.
b. Any documents relating to an administrative or criminal investigation, trials, tenders or general financial or economic affairs, unless the disclosure of the context thereof is permissible.
c. Military intelligence reports, unless they fall within another higher classification.
d. Reports which, if disclosed, may demoralize the citizens unless its publication is permitted.
e. Military wireless frequencies of the armed forces, security forces, public intelligence or any other governmental authority.
f. Any other information or protected document that harms the reputation of any official or impairs the standing of the State.

Finally, Article 10 classifies all other official documents, not included in the above classifications, as 'ordinary' documents which may not be disclosed to "non-concerned persons … unless permitted for publication."

Analysis

The classification scheme contains numerous serious shortcomings. We are particularly concerned by Article 10 which purports to impose classification upon all official documents without any reference to national security concerns. Articles 3, 6 and 8 delineate the three levels of 'protected secrets or document'; however, as outlined above at Section 3.2, the Law is not clear as to what constitutes 'protected secrets or document.' The result of this is that any information that a state official decides to classify may be deemed 'protected'.

The system for classifying information is a restriction on access to information. Restrictions on access to information are permissible only if they serve the legitimate aims delineated in the ICCPR. These aims are limited to the rights and reputations of others, national security, public order, and public health and morals.

As stated in Section 2.2.2, above, Principle 12 of the Johannesburg Principles warns that States 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." This requirement necessitates that restrictions be narrowly drawn.

The categorization in Article 10 of all other official documents as 'ordinary' provides that information may not be disclosed to non-concerned persons unless permitted for publication. Article 10 is overbroad since it effectively protects all State information. The Law provides no guidelines as to who or how the decision is to be made in regard to whether 'ordinary' information will be permitted for publication or who are non-concerned persons. Furthermore, the determination that "non-concerned persons" are not entitled to access 'ordinary' official documents strikes at the core of the right of access – it reverses the onus of the presumption of disclosure and, in particular, seriously restricts the right of access of the media and other actors who disclose information in the public interest. We urge the removal of this provision.

Many of the categories contained in Articles 3, 6 and 8 impose a blanket exemption for information related to national security. This is fundamentally inconsistent with the requirements under international law for access to information. The liberal use of the term "any information" fails to meet the requirements of drawing the restriction as narrowly as possible and building in a 'risk of substantial harm test'.

Stringent harm tests are necessary in order to prevent abuse in a state secrets regime. In relation to Articles 3, 6 and 8, there is no provision made for the assessment of the time-sensitivity of the information for the protection of national security. Quite often, information which might be properly considered sensitive to national security will no longer be so in two years time. This is one reason why there must always be a separate consideration of whether disclosure would pose a substantial risk to the protected interest, rather than just a blanket exemption for categories of information.

Article 8 is particularly concerning because it provides the broadest restrictions on access to information and also seeks to exclude information on the basis of interests ancillary to national security. While national security is a legitimate protected interest, protecting a State from "embarrassment", causing "administrative or economic difficulties", "documents relating to administrative or criminal investigation, trials, tenders or general financial or economic affairs", reports which "may demoralize the citizens" or "information…that harms the reputation of any official or impairs the standing of the State" are not necessarily so. It is fundamental to open government that they, and their officials, are subject to comment and criticism and that the functioning of government agencies are open to the scrutiny of the public. It is unjustifiable to consider these to be issues relating to national security.

Article 3(b) is overly broad because it allows for the classification of all internal security measures, whether economic, production, supply, construction or transportation, regardless of whether disclosure of the information poses a threat to national security. Article 3(b) should include a harm test to determine whether information may pose a serious threat to military operations or internal security. Only information that poses such a threat should be classified as protected. Otherwise, the government would be able to restrict access to almost all information related to the military and public security.

Articles 3(c) and 3(d) also are very broadly drafted and fail to include a harm test. Article 3(c) includes a broad range of information in which there potentially is a strong public interest in disclosing. If it was intended that only inter-state negotiations relating to the drafting of such documents should be excluded from disclosure, this should be stated with more clarity. The public is entitled to access to information concerning international agreements, foreign affairs and military intelligence unless the disclosure would pose a serious threat to national security. Similarly, Article 3(d) prohibits the disclosure of any information "relating to" "general intelligence" or "persons" connected with intelligence. This would extend to the publication of even the name of the person heading up the intelligence services. This provision needs to be replaced with a more specifically-targeted provision protecting material the disclosure of which would have a significant impact on national security.

Article 6(a) imposes a partial harm test by protecting information that would pose a threat to the security of the State. However, the provision is overly inclusive since it also allows information to be classified as confidential on the basis of damaging unspecified State 'interests' or benefiting any foreign state or any other party. This is easily abused to protect

the interests of the government, for example by 'hiding' any information that is potentially damaging to it. In addition, the threshold test for the sensitivity of the documents in Articles 3 and 6 are too vague to properly determine whether a document falls within the classified category. They are inadequate standards to determine what information should be classified to legitimately protect national security. A much more narrowly and precisely worded standard should be imposed.

3.3.2 Persons responsible for classifying information

The Law fails to identify who is responsible for classifying information. Article 19 of the Law states that the "Prime Minister and Ministers are charged with the implementation of the provisions of this Law", however, the Law is not clear as to whether the Ministers must promulgate regulations concerning who shall have the authority to classify information.

Analysis

The failure to specify who is responsible for classifying information is a serious problem in the Law. The Law appears to grant full discretion to any person who has access to official information to classify information. If this were the case, the potential for abuse would be boundless as numerous persons would have the power to classify information. In addition, the Law fails to require that those with the power to classify information possess certain qualifications. The effect of this Law is to allow numerous persons to classify information without any limits on how the decisions are to be made.

Further, even if it were proposed that the Ministers identify the persons with responsibility for classification of information, this is according excessive discretion on an issue which is critical to the protection of the right to access information. We consider that only Ministers and designated senior officials should have the authority to classify information and the appointment procedure should be set out in the Law, with appropriate criteria and safeguards for accountability of this decision-making role. The protection of national security is not such that this process be shrouded in secrecy.

Recommendations:

- Article 10 providing for the classification of "ordinary" information should be removed.
- Articles 3, 6 and 8 should be amended significantly to reduce the list to include only internationally recognised legitimate interests. The list of protected categories should be more narrowly and clearly drawn.
- The definitions of classifiable protected information should be amended to include stringent harm tests that require the harm to relate directly to specific legitimate interests.
- The Law should limit the power to classify information to Ministers and designated senior officials and the Law should explicitly state their process of appointment and include appropriate procedural safeguards.

3.4 Consideration of overriding public interest in disclosure

The Law fails to provide for disclosure even when the public interest in disclosure outweighs the state's need for protection. As recognised by the Johannesburg Principles, no person shall be punished for the disclosure of information if "the public interest in knowing

the information outweighs the harm from disclosure."[29] This is also recognised in the Special Rapporteurs 2004 Declaration on Freedom of Information and Secrecy Legislation.[30] It is integral to the proper functioning of government that the broader public interest in disclosing the information is always considered. Frequently, public disclosure of such information is necessary in order to bring about reform in State organizations. Also, there is often a significant public interest in the disclosure of the information for a wide range of other legitimate reasons. These must be accommodated rather than adopting a closed door attitude to all information which may tangentially touch upon sensitive issues of security, for example, or economic policy.

Recommendation:

- The Law should include a public interest override, allowing for the disclosure of information when the public interest in disclosure outweighs the potential harm from disclosure.

3.5 Review Mechanism for Classification of Information

The Law fails to provide for a review mechanism which means decisions to classify information are never subject to review. Therefore, the potential for abuse is great since every decision is final once it is made. Principle 1.1(b) of the Johannesburg Principles states "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."

The Law also fails to allow for changes in the classification of information. This failure is a serious shortcoming as information, once classified as protected, will remain protected indefinitely. Persons could wrongfully classify information as protected knowing that the decision would never be revisited and the information would remain protected forever. This has particular impact in regard to the time-sensitivity of the information in the assessment of harm to national security.

The review mechanism should provide for regular review of all classified information to assess whether or not ongoing classification remains necessary. Qualified persons other than the person who originally classified the information should conduct the review. The Hungarian classification law provides for review every three years and the Bulgarian law provides for review every two years.[31] We recommend a similar timeframe in this case. All categories of information should be subject to obligatory review for re- or de- classification, as well as the classification determination was justified in the first place.

Recommendations:

- All decisions to classify information should be subject to independent review.
- A provision providing for a formal review mechanism of protected information should be added.
- Qualified persons other than the person or persons who originally classified the information should complete the review of classified information for re- or declassification.

[29] Principle 15.
[30] See Note 4 above.
[31] See *Memorandum on the Law of the Republic of Uzbekistan on "Protection of the State Secrets",* Article 19, June 2004.

3.6 Whistleblowers

The Law should provide protection for whistleblowers who release classified information, if the disclosure was made in good faith and with a reasonable belief that the information was substantially true and disclosed evidence of wrongdoing. Protection for disclosure in the public interest should extend to employees who come across protected material that discloses wrongdoing, if they release the information in good faith. ARTICLE 19 has also recommended the inclusion of protection for whistleblowers in the draft freedom of information legislation which is currently before the Jordanian parliament.

Wrongdoing should include the commission of a criminal offence, failure to comply with a legal obligation, a miscarriage of justice, corruption or dishonesty, or serious maladministration regarding a public body. Protection should also be granted to those who disclose information relating to a serious threat to health, safety or the environment, regardless of whether the information is linked to individual wrongdoing. Protection for whistleblowers encourages accountability in the government sector.

Protecting whistleblowers is fundamental to the operation of open and accountable government and is a standard provision in freedom of information legislation in a wide range of countries. In addition, the Special Rapporteurs 2004 Declaration on Freedom of Information and Secrecy Legislation stresses the need for information 'safety valves' such as whistleblowers and calls for the protection of those who disclose information so long as the person acted in good faith.

The role of whistleblowers in this regime is particularly important given the current lack of provision for review or declassification. Further consideration needs to be given to promote protection of whistleblowers in the face of the severe criminal sanctions within the Law which apply to those people who disclose classified information. It is a difficult balance to strike, but a significant one for the protection of basic fundamental rights. The provisions relating to the protection of whistleblowers needs to be drafted in the context of amending the provisions relating to the criminal sanctions within the Law, as outlined below at Section 3.7. In particular, the strict liability nature of the offences poses a real threat to any persons risking to speak out about classified information.

Recommendation:

- The Law should provide protection to whistleblowers who act in good faith and with a reasonable belief that the information was substantially true and disclosed evidence of wrongdoing.

3.7 Criminal sanctions

Article 14 imposes criminal liability on "any person who has entered or attempted to enter a restricted place for the purpose of accessing secrets, items, protected documents or information that must remain secret to endure the security of the State." The person "shall be sentenced to temporary hard labor." This provision further states that "[i]f such an attempt is made for the benefit of a foreign State, he shall be sentences to hard labor for life. If the foreign State was an enemy, he shall be sentenced to death."

Article 15 stipulates that anyone who "steals" classified information shall be subject to hard labor for a minimum of ten years. If the information was obtained for the benefit of a foreign State, the penalty is hard labor for life. If it is an enemy foreign State, the person shall be sentenced to death.

Article 16 imposes criminal liability on any person who discloses, without a legitimate reason, any protected information which he obtained through his position in a Department. He shall be sentenced to hard labor for a minimum of ten years. If he discloses the information to a foreign State, the sentence is hard labor for life. If it was an enemy foreign State, he shall be sentenced to death.

Analysis
The criminal sanctions for attempting to or accessing protected information are excessively severe. Such harsh sentences in and of themselves constitute a violation of the right to freedom of expression.[32] As noted in Principle 24 of the Johannesburg Principles, "[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." Article 14 is particularly problematic in this regard. These penalties exert a serious chilling effect on the discovery of information in which there is a strong public interest in being disclosed.

The severity of the sanctions is intensified by the strict liability nature of the offences, with the exception of Article 16(a) which allows a limited and subjective qualification of holding a "legitimate reason". Strict liability is not compatible with the right to access information or the legitimate protection of whistleblowers. These provisions have a wide-ranging application, with a particularly harsh impact on those who seek to disclose information in the public interest. The provisions should reflect this, factoring in why the information may have been sought and what its intended use was. The provisions should be narrowly drafted offences which clearly link harm to national security to the proscribed conduct and which impose sanctions which are proportionate to the crime in the circumstances. At a minimum, there should be an appropriate degree of discretion available to sentencing for an offence under Articles 14 to 16.

It is also important to note that the legitimacy and scope of these provisions hangs on the definition of "protected secrets and document", as do a number of provisions in the Law. We reiterate the importance of ensuring that this definition is drafted appropriately narrowly to reflect the purpose of protecting national security within the acceptable boundaries relating to harm and public interest disclosure.

Recommendations:
- The Law should be amended to provide for proportionate sentences for the crimes.
- The Law should clearly and specifically describe the offences.

3.8 Lack of sanction for wilful misclassification of information

The Law fails to provide a sanction for the willful misclassification of information. The Law should provide sanctions for the intentional misclassification of information for purposes of breach of the law, corruption or to limit the public's access to information. In order to effectively prohibit the misclassification of information, the Law must provide such sanctions.

[32] See, for example, *Tolstoy Miloslavsky v. United Kingdom*, 13 July 1995, Application No. 18139/91 (European Court of Human Rights).

Recommendation:

- The Law should provide sanctions for the wilful misclassification of information.