NATIONAL SECURITY AND THE RIGHT TO INFORMATION

PARIS 11TH DECEMBER 2012

Sandra Coliver,
Senior Legal Officer, Freedom of Information & Expression
Open Society Justice Initiative
http://www.right2info.org/exceptions-to-access/national-security
Sandra.Coliver@opensocietyfoundations.org

I thank the Committee for this opportunity to discuss the draft Global Principles on National Security and the Right to Information (RTI), being drafted by my organisation, the Open Society Justice Initiative, in close consultation with experts around the world.

Today I will describe briefly:

- the reasons my organization decided to lead a process to draft these Global Principles;
- the aims we hope these Principles will serve;
- the process of extensive consultation that has led to the current draft; and
- the process still to be completed to finalize the Principles.

I will then highlight some of the key aspects of the Principles; and I will offer some of the results of a survey conducted by an academic at the University of Copenhagen concerning the law and practice of twenty Council of Europe member states concerning these key issues.[1]

1. BACKGROUND: REASONS FOR DRAFTING THESE PRINCIPLES

In 1995, when I served as the Law Programme Director of Article 19, the Global Campaign for Freedom of Expression, based in London, I coordinated a similar effort that resulted in a set of global principles known as the Johannesburg Principles on National Security, Freedom of Expression and Access to Information.[2] Those Principles were welcomed and circulated by the UN Rapporteur on Freedom of Expression, were translated into more than a dozen languages, and were widely cited, including by courts, academics, NGOs and government officials. UN offices continue to transmit these Principles to governments when requested to provide advice concerning the drafting of laws, regulations or policy concerning the classification of information.

My organisation decided to update the Johannesburg Principles in response to requests from experts in several countries who contacted us for advice on global best practices to help in drafting or revising laws and policies regarding the withholding of information from the public on national security grounds. The number of requests for such assistance was growing for several reasons.

First, more than 80 countries – includin the population giants of Brazil, China, India, Indonesia and Russia – have adopted access to information laws since the fall of the Berlin Wall, and are, for the first time, grappling with how to keep information secret pursuant to law, whereas previously decisions as to whether to disclose information were completely discretionary.[3] Thirty-six of the member states of the Council of Europe adopted access to information laws since 1989.[4]

---

[1] The 20defence countries studied are Albania, Belgium, Czech Republic, Denmark, France, Germany, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Romania, Russia, Serbia, Slovenia, Spain, Sweden, Turkey, and the United Kingdom. We expect to receive questionnaires from the following five additional member states: Bulgaria, Croatia, Estonia, Georgia and Ireland. The names and qualifications of the experts who completed the questionnaires are listed in an annex to these remarks.

[2] *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information* at http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf. *See* Coliver, et al (eds.) *Secrecy & Liberty* (Martinus Nijhoff Pubs 1999), which includes 30 papers on national and international law and practice, including a commentary, principle by principle.

[3] As of November 2012, 93 countries had national laws or judicially enforceable regulations conferring the right of access to information, at least in law, to more than 5.2 billion people.

[4] These include the 47 member states, less Andorra, Cyprus and Monaco, and the eight members that adopted their laws before 1989, namely: Austria 1987, Denmark 1985, Finland 1951, France 1978, Greece 1986, Netherlands, 1978, Norway 1970, and Sweden 1766.

Second, while all of these laws allow state agents to withhold information from the public on grounds of national security and/or closely related grounds of state or internal security, few of the laws, or their implementing regulations, define national security for purposes of withholding information. Nor do they set froth clear standards or procedures for

- classifying or otherwise withholding information on security grounds;
- encouraging the proactive disclosure of information of high public interest;
- making clear the categories of information that should be available to independent oversight bodies and the courts tasked with overseeing the handling of national security information;
- protecting whistleblowers; and
- punishing unauthorised disclosures.

Third, the rise in terrorist attacks provided an impetus for many governments to enhance their secrecy regimes and increase secret surveillance.

Fourth, and relatedly, NATO issued a new information policy in 2002 that requires member states and states seeking membership to institutionalise and tighten their systems for handling national security information.[5]

Fifth, the WikiLeaks disclosures brought world attention to the challenges of keeping information from the public and raised questions about best practices for identifying and safeguarding information that genuinely needs to be kept from public scrutiny.

2. AIMS OF THE PRINCIPLES

To respond to the above needs, my organization invited experts to help draft Principles.

We agreed that the Principles should 1) be practical – meaning that they should not impose undue burdens on those tasked with implementing them – and b) reflect best practices. All Principles are supported by the actual practice of one or more countries, and/or by clear statements of international hard or soft law.

As a whole, the Principles reflect international and national law and standards, evolving best practices, and the general principles of law recognised by the community of nations.

A key premise of the Principles, set forth in the first preambular paragraph, is that both the public's right of access to information and the ability of the state to protect national security, including through secrecy when strictly necessary, are vital to a democratic society, and are essential for its security, progress, development, welfare, and the full enjoyment of human rights and fundamental freedoms.

3. PROCESS

In order to gather support for the Principles, we invited experts to undertake research, write papers, and complete detailed questionnaires on the law and practice of their countries concerning key issues.[6]

We are in the process of drafting a Commentary that will set forth support for each principle, based on the papers, survey results and other expert research.

The draft Principles, papers in support of them, and groups with which we are working are set forth at this website: http://www.right2info.org/exceptions-to-access/national-security.

[5] Security Within the North Atlantic Treaty Organisation, Doc. C-M(2002)49, adopted 26 March 2002, issued 17 June 2002, including Enclosure E on Security of Information and Enclosure F on INFOSEC, as revised by the Directive on Security of Information, Doc. AC/35-D/2002-Rev2, issued 4 Feb 2005.

[6] We have collected detailed questionnaires from experts in the following 20 Council of Europe member states: Albania, Belgium, Czech Republic, Denmark, France, Germany, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Romania, Russia, Serbia, Slovenia, Spain, Sweden, Turkey, United Kingdom. We are in the process of obtaining questionnaires from experts in several other European countries.

We have now held regional meetings all over the world:

- Jakarta (with participation of experts from 15 Asian countries),
- Buenos Aires (with experts from 10 Latin American countries),
- Budapest and Copenhagen (with experts from 26 European countries),
- Dar es Salaam (with experts from 8 countries in eastern Africa),
- Dakar (with experts from 10 countries in west and central Africa)

We also held national-level meetings in Cape Town, Delhi, London and Washington DC, and we plan to hold a meeting in February in Johannesburg for experts from 10 countries of Southern Africa.

Most of the meetings were hosted by academic institutions; a few were co-hosted by state bodies. Participants included former and current government officials, academics, civil society experts, information commissioners, and inter-governmental experts.

These have included the current and former UN Special Rapporteurs on Counter-Terrorism and Human Rights (Ben Emmerson and Martin Scheinin), and the four special mandates on freedom of expression:

- the UN Special Rapporteur on Freedom of Opinion and Expression, Frank LaRue;
- the OSCE Representative on Freedom of the Media, Dunja Mijatovic;
- the OAS Special Rapporteur on Freedom of Expression, Catalina Botero; and
- the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, Pansy Tlakula.

Several of these experts have expressed an interest to devote parts of their reports to the issue of national security and the right to information, and to formally endorse or welcome the Principles.

Attached is a list of the European experts who have contributed to the drafting of the Principles.

In addition, we have been working closely with three key partner organisations:

- Amnesty International,
- the International Commission of Jurists, and
- the Geneva Centre for the Democratic Control of the Armed Forces (which worked closely with Special Rapporteur Martin Scheinin in developing the "UN good practices on legal institutional frameworks for intelligence services and their oversight"[7]).

The draft before you thus represents the work of some 400 experts from 73 countries who met at a total of nine meetings in 2011 and 2012.

We are continuing to fine-tune the Principles in order to achieve maximum consensus and, to the greatest extent possible, produce Principles that 1) appropriately balance the sometimes competing rights and interests of national security, access to information, the right to information about human rights violations, and personal privacy; and 2) are relevant for all democratic societies.

A drafting committee with members from all regions and a variety of backgrounds and perspectives is now working to finalise the Principles. We aim to produce a final draft by mid-March.

4. REQUIREMENTS THAT ALL RESTRICTIONS ON ACCESS MUST MEET

Several of the Principles reflect general standards that all exceptions to the right of access to information must meet in order to comply with international law and standards. There is now widespread consensus concerning these requirements as reflected in the Council of Europe Convention on Access to Official Documents, the Model Laws of the Inter-American System and the African Union, the UN Human Rights Committee General Comment on Article 19, and judgements of regional and national courts.

[7] UN Doc. No. A/HRC/14/46, issued 17 May 2010.

1) Disclosure is the rule, and any exception should be as narrow as possible to protect a legitimate interest – this is called the principle of maximum disclosure, and is set forth in Principle 1.
2) Where a document or other record contains some information that may be kept secret, only that information may be withheld and all the rest should be disclosed – this is called the duty to segregate. (See Principle 24)
3) For an interest to legitimately justify withholding, it must be clearly defined in law and must be among those interests recognised as legitimate under international law – the principles of legitimacy and legality. (Principle 3)
4) For a restriction on the right to information to be necessary in a democratic society, a disclosure must threaten to cause substantial harm to a legitimate interest – this is known as the harm test. (Principle 3)
5) The harm must be greater than the public's interest in having the information – this is known as the public interest test, or public interest override, which is understood to be part of the principle of necessity as applied to restrictions on the right to information. (Principle 3)
6) The public authority seeking to withhold the information bears the burden of establishing points 3, 4 and 5, above. (Principle 4)

4.1 THE PUBLIC INTEREST OVERRIDE

A study by an Irish law professor of 93 RTI laws, virtually all in the world, found that 44, or a little less than half, contain an express public interest override concerning at least certain exceptions.[8] Most of the countries that do not have a public interest override passed their RTI laws before the late 1990s; since then, the trend has been to include a public interest override and for the override to be mandatory (meaning that upon a finding that the public interest in disclosure outweighs the likely harm, the information *must* be disclosed). Moreover, modern laws apply the override to an ever growing number of exceptions: 16 countries – including Belgium, Bosnia and Herzegovina, Moldova, Montenegro, and Ukraine – have laws that apply the public interest override to all exceptions.

Many laws set forth specific categories of information that may never be withheld. For instance, the laws of several Latin American countries – including Brazil, Guatemala, Mexico, Peru and Uruguay -- expressly state that information about human rights violations may never be withheld. Several countries in Eastern Europe have laws that state expressly that information about corruption and other government wrongdoing may not be withheld, the laws of still other countries include a similar – albeit weaker - formulation that information may not be withheld if the *purpose* is to conceal corruption or other wrong-doing.

4.2 ADDITIONAL REQUIREMENTS

In addition, there is international consensus concerning the following points:

Reasons for Refusal and Right to Appeal

1) The reasons for denying information must be set out in writing, and must identify with precision the harm to a legitimate interest that is feared.
2) A requester has the right to a speedy and low cost or free review of a refusal to disclose information, including of an implicit or silent refusal, or of related matters, including fees, timelines, format, etc., by an administrative authority independent of the authority that denied the information request, as well as by a court. The reviewing public authority should have full access to all relevant information.

Procedures for Withholding Information

3) The public should have access to, and an opportunity to comment on, the written procedures and standards governing classification or other withholding.
4) The identity of the official responsible for a decision to withhold information should be indicated on the document, or otherwise be traceable, so as to ensure accountability.

[8] Prof. Maeve McDonagh, University College Cork, Ireland, The public interest test in FOI legislation (2012).

5) Each public body should create, and update annually, a list of the confidential records it holds, save for those exceptional documents whose very existence is legitimately classified. This list should be available to the public.
6) Upon receipt of a request for information, a public authority should confirm or deny whether it holds the requested information, except in extraordinary circumstances in which the very existence or non-existence of the information may be kept secret on national security grounds

4.3 INFORMATION OF ESPECIALLY HIGH PUBLIC INTEREST

Some categories of information should never be withheld. Principle 10 states that this is so, "in particular, [concerning information] regarding [gross] violations of human rights or serious violations of international humanitarian law" and "laws, [primary] regulations and policies" concerning human rights and humanitarian law violations; military, police, security and intelligence authorities; and all forms of secret surveillance and systems of secret files and registers.

The public has an especially high interest in certain other categories of information listed in Principle 10; public authorities should proactively disclose such information, and concerning such information, a public authority will carry a particularly heavy burden to demonstrate that secrecy is necessary.

Categories of information of especially high public interest include, but are not limited to, information the public needs in order to:

- enjoy their rights and access their entitlements fairly, without discrimination or arbitrariness -- including all laws, policies and regulations;
- protect their health and safety including information about pollution, emissions, emergency response plans and threat levels;
- Prevent maladministration or corruption, including information about the expenditure of public funds;
- exercise democratic oversight;
- participate in public affairs, including information about candidates for office, elections, votes of legislatures, decisions of public officials.

5. KEY ASPECTS OF THE PRINCIPLES AND SUPPORTING RESEARCH

In developing these Principles, the Justice Initiative invited experts to write thematic papers that compile international law and best practices on key topics and national papers that examine a range of issues within a single country context. The papers that have been double-checked and edited are posted on our website: http://www.right2info.org/exceptions-to-access/national-security.

In addition, we asked Amanda Jacobsen, a Research Fellow at the University of Copenhagen, to conduct a survey of the law and practice of 20 Council of Europe member states (hereinafter called "the European Survey). Questionnaires were completed by experts in each of 20 countries.[9] Dr. Jacobsen is currently in the process of double-checking all of the information and, thus, the figures presented here may shift somewhat as the result of further research.

The below sections offer a snapshot of some of the key findings and the Principles that relate to those findings.

5.1 DEFINITION OF NATIONAL SECURTIY AND ACCESS TO INFORMATION

The European Survey found that in 65% (13 out of 20)[10] of the member states surveyed, national security is not defined in law for the purposes of justifying non-disclosure. In five of these countries,

[9] The countries, names of the experts, and brief biographical statements are included in an annex.
[10] Experts from the following 12 countries expressly stated that no definition is provided in their country's national law for the purposes of justifying the non-disclosure of government-held information: Belgium, Denmark, Hungary, Italy, the Netherlands, Norway, Russia, Serbia, Slovenia, Spain, Sweden, and the United Kingdom. The Turkish expert implied that Turkish law also does not include a definition.

some definition is provided in legal provisions other than those relating to the handling of information.[11] Experts from three countries (Belgium, Denmark and Russia) expressly stated that the law of their country provides no definition at all.

Given that there is no international consensus, and that what constitutes national security or closely related terms such as "internal security" or "state security" varies from state to state, the drafters of the Principles decided not to include a positive definition of national security.

Rather, Principle 2 simply states that "It is a good practice for national security to be defined precisely in the constitution or a law."

This is the same approach recommended by UN Special Rapporteur Martin Scheinin, in his "Good Practices" document: "While the understanding of national security varies among States, it is good practice for national security and its constituent values to be clearly defined in legislation adopted by parliament … ."[12]

In addition, because of strong expressions of concern at regional and national consultations regarding the potential for abuse of rights as a result of overbroad definitions of national security, we decided to include the following negative definition in the Definition section of the Principles.

> **"Legitimate national security interest"** refers to an interest the genuine purpose and primary impact of which is to protect national security, consistent with international and national law. A national security interest is not legitimate if its genuine purpose or primary impact is to protect an interest unrelated to national security, such as protection of government or officials from embarrassment or exposure of wrongdoing; concealment of information about human rights violations, any other violation of law, or the functioning of public institutions; strengthening or perpetuation of a particular political interest, party or ideology; or suppression of lawful protests.

5.2 FOCUS ON THE PUBLIC'S RIGHT OF ACCESS TO INFORMATION

We decided to focus the Principles on the public's right to information, and to address the rights to information of detainees, those accused of crimes, victims of human rights violations and others with heightened claims to information only to the extent that those rights are closely linked with the public's right to information and open justice. Preambular paragraph 15 notes this focus. These Principles are not intended, and should not be understood, to limit in any way the rights to which detainees, the criminally accused, human rights victims and other groups with special information claims are entitled.

5.3 JUDICIAL OVERSIGHT (Principles 29-33)

The Principles on Judicial Oversight seek to ensure that national security claims do not:

- undermine the fundamental principle of open justice,
- prevent victims of human rights violations from pursuing their right to an effective remedy,
- prevent those accused of crimes from knowing the evidence against them,
- preclude courts from reviewing evidence necessary to make fair decisions, or
- interfere with the right of an individual to have a court review the denial by a public body of a request for information, even if classified.

[11] Italy ("Italian law does not provide for an explicit definition of 'Security of the Republic.' However, specifically regarding the state secrets privilege, this definition can be easily and clearly deduced from article 39.1 of Law 124/2007"); Sweden (referring to a definition for crimes against national security provided in the Criminal Code); Hungary (referring to a definition of national security provided in Act CXXV of 1995 on National Security Services "for purposes of that act"); Spain (referring to a definition of national defence contained in the National Defense Act of 2005); and the United Kingdom (noting that there is an incomplete definition of national security reflected in the Security Service Act 1989).

[12] See Scheinin's Good Practices, note to Practice 1, *supra*, note [_].

The European Survey uncovered several trends that support these Principles, and also illustrate some of the problems that the Principles seek to address.

For instance, the survey found that all 20 of the countries surveyed provide judicial review for denials of information requests. 11 also provide a speedy, low-cost administrative procedure for review of such denials.[13]

In 19 of the 20 countries (all save France), the courts have the authority to examine classified information (although in some countries, this authority is limited to specialised courts or judges with security clearances).

Experts in 15 of 18 (83%) countries stated that judges have the authority to order the release of information if they determine that information does not need to be kept secret, despite a public authority's assertion that national security justifies withholding the information.[14]

Nonetheless, an overwhelming majority also indicate that judges normally defer to the assertions of government officials that disclosure would harm national security.

In all of the 20 countries, judicial decisions are required to be made available to the public, subject to redactions to protect privacy interests. 13 of 16 experts to address the issue stated that in their countries, national security cannot justify withholding an entire judicial decision.[15]

In all 20 countries, court hearings and trials are presumptively open to the public. However, in Russia and the UK, it is possible to keep a court case entirely secret, such that it is not even recorded on the public's docket.

In 85% of the countries, a court may not dismiss a case without reviewing the case on its merits, even when a public authority asserts that such review would require scrutiny of state secrets.

At least two of the states – France and Romania -- provide that all evidence that forms the basis of a criminal conviction must be made available to the public, although in some cases, testimony may remain anonymous. In 12 of 19 countries,[16] all evidence that forms the basis of a criminal conviction must be made available to the accused, including in cases involving national security.

5.4 WHISTLEBLOWERS (Principles 39-47)

Principles 39-45 address protections for public personnel who disclose information. These Principles call on states to:

- Establish or designate bodies independent of the security sector to receive and effectively investigate complaints from security sector personnel concerning wrongdoing, significant mismanagement or waste, and dangers to public health, safety or the environment; and
- Encourage employees to submit information, including classified information, to such bodies, and protect them from all forms of retaliation.

Only 30 % (6 of 20) of the states surveyed have whistleblower laws that apply to personnel in the security sector.

[13] The eleven are France, Germany, Hungary, the Netherlands, Norway, Poland, Serbia, Slovenia, Sweden, Turkey, and the United Kingdom.
[14] The 15 are Czech Republic, Denmark, Germany, Hungary, Italy, Moldova, the Netherlands, Romania, Russia, Serbia, Slovenia, Spain, Sweden, Turkey, and the United Kingdom. France and Norway did not provide a response.
[15] The three countries in which national security may justify withholding an entire court decision are Norway, Russia, and the UK.
[16] These are Czech Republic, France, Germany, Hungary, Italy, Moldova, Netherlands, Romania, Russia, Slovenia, Spain, and the UK.

In 5 out of 20 states, whistleblower laws protect disclosures of certain categories of classified information pertaining to government wrongdoing.[17]

Only 5 states have established an independent body to receive complaints involving classified information.[18]

In several countries, public personnel are encouraged to make internal complaints; in some countries public personnel are obliged to report criminal wrongdoing. However, in several countries, there are only very limited protections against retaliation.

Principle 46 sets forth the limited situations in which a public servant may disclose classified information to the public. This Principle has been the subject of considerable discussion and is still being revised. Basically, the Principle seeks to provide protection from criminal prosecution, though not necessarily from other penalties (dismissal, loss of security clearance, etc) when all of a series of conditions are met. These include the following:

- The disclosure concerns the commission of a serious crime (including human rights violations) or a matter that is of immediate and serious harm to public health, safety or the environment [or significant mismanagement or waste];
- The extent of the disclosure was necessary to disclose the aforementioned matters;
- the public servant (i) already made the disclosure through internal procedures; *or* (ii) has reasonable grounds to believe that disclosure through internal procedures or to an independent oversight body would result in evidence being concealed or destroyed or has (or could) result in retaliation against him/her or any other individual; and
- the harm or risk of harm created by disclosure is outweighed by the importance for the public of access to the information.

That Principle seeks to encapsulate the essence of the 2008 decision of the European Court of Human Rights in the case of *Guja v. Moldova*,[19] and also reflects the law of Canada.[20] It goes further than the law of most of the Council of Europe's member states, but it is consistent with an emerging trend of actual practice.

All of the states in the European Survey provide that public personnel may be criminally charged for disclosing classified national security information. The maximum penalty for this crime varies from 2 years to life imprisonment; however, where there is no espionage, treason or disclosure to a foreign state, the penalties are generally less: up to 2 years in Denmark and the UK; 4 years in Spain and Sweden; 5 years in Belgium, Germany, Poland and Slovenia; and 7 years in France.

In most states (other than Albania, Belgium, Norway, Romania, Spain and Turkey), at least one public servant has been criminally charged for disclosure to the public of classified information in the last two decades. Other than Germany (where some 200 public servants have been prosecuted), in most states only a handful have been prosecuted and even fewer have been convicted. However, in Russia, 10 public servants were convicted and sentenced for terms ranging from 4 to 15 years for the public disclosure of information.

Most states (Albania, Czech Republic, Germany, Italy, Moldova, the Netherlands, Norway, Romania, Spain, and Sweden) require a showing of either actual or probable harm resulting from the disclosure in order for a penalty to be imposed. Of those that do not require such a showing, at least 3 (Hungary, Denmark, and France) allow the lack of harm to be raised as a defence or mitigating circumstance.

In 6 countries (Albania, Germany, the Netherlands, Romania, Serbia, and the United Kingdom), the fact that a public servant used, or tried to use, internal reporting procedures before making the information public, may constitute a defence.

---

[17] These countries are Hungary, Romania, Serbia, Slovenia, Sweden. However, as concerns Hungary, although there is a general whistlblower protection law, it cannot be enforced, as the authority responsible for its enforcement has not been established or designated.

[18] These are Belgium, Hungary, the Netherlands, Serbia, and the United Kingdom.

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

[20] *Security of Information Act* (R.S.C., 1985, ch. O-5).

5.5 DISCLOSURES OF CLASSIFIED INFORMATION BY THE MEDIA AND OTHER MEMBERS OF THE PUBLIC (Principle 50)

Principle 50 states that members of the media and other persons who do not have authorised access to classified information may not be punished for disclosing information to the public except when disclosure actually resulted in serious [physical] harm, and the person who disclosed the information reasonably should have known that such harm was likely.

The precise language of this Principle is still being revised to reflect the appropriate balance between safeguarding the role of the media as a public watchdog and deterring the publication of information that knowingly, and perhaps intentionally, causes harm. The Principle finds some support in the law of Council of Europe member states.

At least 3 states (Belgium, Germany, Moldova) do not provide criminal penalties for mere disclosure of classified information by the media or other persons without authorised access to that information, although at least in Germany, it is a crime for members of the media to "instigate" a violation of official secrets.

In several of the states that do penalise persons without authorised access for disclosure of classified information, public interest considerations may constitute a defence.

Only rarely in the last two decades have members of the media been charged for the disclosure of classified information, and in none of these cases has a member of the media served time in prison.

CONCLUSION

In closing, although today I focused on our research concerning Council of Europe member states, I wish to emphasise that we also have undertaken research concerning countries in the Americas, Africa and Asia. The Global Principles we are drafting reflect international law and global best practices and are intended to be universally applicable.

They are not intended to be, for instance, a set of indicators by which to gauge the performance of countries. Nor are they a set of binding obligations.

Rather, they are intended to be a resource for people who are engaged in developing or revising laws or policies concerning national security and the public's right to information.

The hope of the drafters is that these Principles will help people in countries grappling with these vexing challenges, many for the first time, to set down legal and policy frameworks that will promote improved democratic oversight of national security information and thereby encourage better informed decision-making; reduce opportunities for hiding corruption and incompetence; improve procedures for safeguarding information whose disclosure would likely cause overriding harm; increase protection of human rights; promote more effective parliamentary and judicial oversight; and enhance genuine security for nations and their people.

Endorsement of these Principles, or some other suitable form of recognition, by this Committee would very significantly enhance their potential to promote improved legal and policy frameworks not only in Europe but also throughout the Americas, Africa and Asia.

I would be pleased to answer any questions you might have.

Thank you for this opportunity.

- end -

DRAFT GLOBAL PRINCIPLES ON NATIONAL SECURITY AND THE RIGHT TO INFORMATION

Changes from the draft of 18 Nov 2012 presented to the PACE Legal Affairs and Human Rights Committee

First preambular paragraph is revised as follows to clarify the point that the paragraph was trying to make:

> ~~*Reaffirming their conviction that*~~ *Recognising* both that the public has a right of access to information and ~~the ability~~ that states can have a legitimate interest in withholding certain information from the public, including on grounds of ~~the state to protect~~ national security, ~~including through secrecy when strictly necessary, are~~ and emphasising that striking the appropriate balance between the two is vital to a democratic society and essential for its security, progress, development and welfare, and the full enjoyment of human rights and fundamental freedoms;

Definitions

- Deleted the definition of "legitimate interest"
- revised the definition of "legitimate national security interest" so that it is purely a negative definition and does not reference Principle 9, as follows:

> **"Legitimate national security interest"** refers to an interest the genuine purpose and primary impact of which is to protect ~~categories of information listed in Principle 9.~~ national security, consistent with international and national law. A national security interest is not legitimate if its genuine purpose or primary impact is to protect an interest unrelated to national security, such as protection of government or officials from embarrassment or exposure of wrongdoing; concealment of information about human rights violations, any other violation of law, or the functioning of public institutions; strengthening or perpetuating a particular political interest, party or ideology; or suppression of lawful protests.

Principle 2 – added the following underlined words so that it now reads:

> "These Principles apply to information held by a public authority where the authority asserts that the release of such information could cause harm to national security, including national security aspects of defence, intelligence activities or international relations of the state."

Principle 9

- Paragraph vi was revised as follows:

> Information concerning the prevention, investigation [or prosecution] of terrorist attacks, subject to ~~safeguards for protecting legitimate privacy interests of suspects and witnesses~~ the rights of victims of terrorism to information about such investigations and prosecutions, and the rights of individuals subject to such proceedings to a fair and public trial and protection against violation of their human rights;

- Paragraph vii – re inventions in which the government has an ownership interest - has been deleted, on the ground that the essence of the paragraph is already covered by paragraph i.

- Paragraph ix was slightly tightened by adding the following underlined word:

> Other similar matters, so long as preservation of their secrecy is necessary to protect a legitimate national security interest that is set forth in law, narrowly drawn, and adopted following opportunity for public comment.

Principle 46, concerning disclosures to the public by persons with authorised access to confidential information, continues to be revised as we continue to try to clarify the categories of "protected

disclosures" that should not be subject to penalty, and the categories of disclosure that may be subject to criminal penalty.

Principle 50 – option B has been deleted. It was a remnant of an earlier draft.

Principle 53 has been revised to include the following underlined words:

> Nothing in these Principles should be interpreted as restricting or limiting any right to information recognised under international, regional or national law or standards, or any provisions of national or international law that would provide greater protection for disclosures of information by public personnel or others.

* * * * *

NATIONAL SECURITY AND THE RIGHT TO INFORMATION:
SURVEY OF LAW AND PRACTICE OF 20 COUNCIL OF EUROPE MEMBER STATES

Expert Contributors

Albania:
Ilir Gjoni, an MP for the Albanian Parliament, has over 20 years of experience in various government and nongovernment institutions. He graduated in 1985 from Tirana University, Faculty of History and Philology and has two Master degrees: one in Diplomacy acquired at the Mediterranean Academy of Diplomatic Studies and the other in National Security Affairs from the Naval Postgraduate School in California. He has worked in diplomacy (MFA) for almost ten years and in journalism as an international news editor in one of Albania's biggest independent newspapers. His working experience also includes acting as a senior government Legislator (2001-2005 and 2009 to date), as well as Chief of Staff to the Prime Minister (1999-2000) and both Defence and Interior Minister (2000-2002).

Belgium:
Frankie Schram has studied history, philosophy, musicology, law, political science and public management. He is member and secretary of the Federal Commission on access to and reuse of administrative documents, member and secretary of the Federal Appeal Commission on the Access to Environmental Information in Belgium and member of the Flemish Supervising Commission of electronic administrative data-exchange. He is also visiting professor at the Public Management Institute of the Faculty of Social Science of the KU Leuven and visiting professor at the Faculty of Political and Social Science at the Faculty of Law of the University of Antwerp. He was for several years the president of the group of experts on access to official documents of the Council of Europe. His research domains are freedom of information, complaint management, participation, regulation management and integrity management.

Czech Republic:

Oldřich Kužílek is a consultant for government openness and privacy, a former theater director, radio presenter, and Czech and Czechoslovak politician for the Civic Forum. He was a deputy for the Civic-Democratic Alliance (ODA), a member of the Deputy Federal Assembly, and later served on the Czech National Council and the Chamber of Deputies.

Denmark:

Pernille Boye Koch is an Associate Professor and lecturer in Constitutional Law at the Faculty of Law, University of Southern Denmark, where she has been since 2004. In 2010, she was a Special Consultant to the Danish Folketing Administration, where she advised on constitutional matters and parliamentary rules. In 2010, she also co-authored a book on the Danish judiciary, entitled *Separation of Powers in Theory and Practice: An International Perspective*. She has published articles, among

others, on freedom of association in Denmark, freedom of religion in Denmark, and on judicial oversight and independence.

France:

Bertrand Warusfel, a Professor at University of Lille II in Paris, teaches European Intellectual Property and Ecommerce Law. He is a member of the Scientific Council of the Institute of Intellectual Property Research Centre, the French Group of International Association for the Protection of Intellectual Property, and the Association of European Patent Practitioners. He is also a member of the Scientific Committee Papers Security, on the editorial board of the journal Intellectual Properties, and the Director of the Association of Sciences-Po. He is the former Scientific Director of the Centre for Security and Defence Research (Faculty of Law of Paris V) and a former member of the committee drafting the French directory of international relations.

Germany:

Eric Töpfer is senior researcher at the German Institute for Human Rights in Berlin, Germany. His research is focused on policing, new surveillance and civil liberties at the domestic and European levels. He has written extensively on video surveillance and European police cooperation, including articles in the European Journal of Criminology, Kriminologisches Journal and Bürgerrechte & Polizei/CILIP.

Nils Leopold is on the Board of Directors of the Humanistische Union, Germany's oldest civil rights organisation, where he previously worked as the Executive Director of the federal chapter. He is also currently the Senior Advisor to Konstantinvon Notz, the spokesperson on interior politics at the German Bundestag in Berlin. Previously, Leopold practiced law in Berlin. Since 2005, he has also been an Officer at the Data Protection Commission of the federal state of Schleswig-Holstein, Germany, from which he is currently on leave.

Hungary:

Ádám Földes of Transparency International has worked in the field of human rights since 2003, conducting research, advocacy and policy development on issues related to access to information, protection of personal data, and state secrecy. Between 2004 and 2008, he led the Freedom of Information and Personal Data Protection Program of the Hungarian Civil Liberties Union. Ádám has engaged in law reform, providing expert opinions at ministerial and parliamentary level, monitoring levels of access to information in practice, and managing strategic litigation and campaigning. He holds a J.D. from ELTE University, Budapest, where he wrote his thesis on video surveillance, and also holds a Master's degree in Sociology from ELTE University.

Italy:

Arianna Vedaschi is an Associate Professor of Comparative Public Law at the University of Bocconi, Faculty of Law. She has her PhD in Legislation Drafting from the Università di Genova and her Masters in Law promoted by Italian Chamber of Deputies, the Italian Senate, and the Faculty of Political Science of Università degli Studi di Firenze. She was previously a researcher in Comparative Public Law and is currently a member of the Regional Board of Electoral Guarantors - Lombardia, Corte d'Appello di Milano. She is also a member of the Faculty Board of the PhD in International Law and Economics. Since 1999, she has been a member of the editorial board of the journal *Diritto pubblico comparato ed europeo*.

Moldova:

Viorel Cibotaru is the Director of the European Institute for Political Studies of Moldova, the Director of the Invisible College of Moldova, and a Senior Associate Fellow of the Center for Democratic Control of Armed Forces in Geneva. He is cofounder of the Documentation and Information Center on NATO, and served previously as its Executive Director. Cibotaru is also a retired lieutenant-colonel of the Moldovan Armed Forces (promoted in 2006 to colonel), and while mobilised, served in the Ministry of Defence as Editor-in-chief of military weekly, Head of the PI and PR office, Head of the

Foreign Relations Department, and Deputy Commander-in-chief of the Moldovan Peacekeeping Forces. From 1980 to present, he has also been teaching Journalism classes at the State University of Moldova.

Netherlands:

Wouter Hins is an Associate Professor of Constitutional and Administrative Law at the University of Amsterdam and a Professor by special appointment of Media Law at Leiden University. In 1991, he was awarded his doctorate by the University of Amsterdam for his thesis on the freedom of reception and foreign broadcasting. He is a member of the complaints committees of the Dutch Media Authority, the Netherlands Public Broadcasting, and the Ministry of Health, Welfare and Sport, and is also editor of the journal Mediaforum and responsible for the quarterly column 'Mediarecht' in Ars Aequi.

Norway:

Ole Henrik Brevik Førland is Senior Legal Adviser for the Norwegian Parliamentary Oversight Committee.

Poland:

Adam Bodnar is a graduate of the Warsaw University (M.A., 2000) and the Central European University in Budapest, Department of Legal Studies (LL.M. in Comparative Constitutional Law, 2001). Since 2006 he is a doctor of laws (Warsaw University). He works as an assistant professor (adjunct) at the Human Rights Chair of the Warsaw University Faculty of Law and Administration. He is also a visiting professor at the Central European University in Budapest. He is mostly interested in the protection of fundamental rights, jurisprudence of the European Court of Human Rights and European Court of Justice, EU citizenship, and the role of NGOs in pursuing public interest and freedom of speech.

Romania:

Codru Vrabie is a trainer and consultant in the field of public administration and public service reform from Romania. He has international experience in non-profit and public management, administrative capacity and institution building, strategic development, fighting corruption and transposing provisions of acquis communautaire. He also has professional training certificates in advocacy and training of trainers. In addition to his native Romanian, he speaks fluent English, understands French, converses in Bulgarian and has a smattering of other European languages.

Russia:

Ivan Pavlov, JD, PhD is the Founder and Chairman of the Freedom of Information Foundation, Russia's largest NGO dealing with FOI rights and governmental openness. Pavlov has authored more than 70 analytical publications on access to official information and governmental openness, and served as an adviser in the drafting and promotion of Russia's FOIA. He serves on a number of advisory boards and is actively engaged in work promoting transparency in government including as a human rights expert for the OSCE. Pavlov was also recently appointed to serve as an expert for the Russian governmental working group on Open Government. A qualified attorney, he has participated as legal counsel in a number of high profile cases on FOI, state secrets, and access to state historical archives.

Serbia:

Marko Milošević is a Researcher and Publications Coordinator with the Belgrade Centre for Security Policy in Serbia. He graduated from the Faculty of Philosophy, Department for Sociology in 2004, obtained his MA degree at the same Department in 2009, and is currently a PhD candidate in International and European Studies at the Faculty of Political Sciences, University of Belgrade. His areas of interest include privatisation of security, multinational operations, new wars, social research, transparency in the security sector, and the defence industry.

Slovenia:

Rosana Lemut Strle has a Master's degree in Law and works with the Information Commissioner of the Republic of Slovenia as Deputy Information Commissioner. Her professional work is now primarily focused on personal data protection and access to public information. Before, she worked at the Health Insurance Institute of Slovenia as Director of the compulsory health insurance section. She is the author of numerous articles from the fields of health insurance and protection of personal data. In both fields, she is also active as a lecturer.

Spain:

Susana Sánchez Ferro is Professor of Constitutional Law at the Autonomous University of Madrid. She is an expert on the right of citizens to access government security information and has a monograph on State Secrets published by the Center for Constitutional Studies, in addition to several articles on the problems posed for a democratic state of law, the tension between national security and civil liberty. She served as consultant to the European Parliament in a study on the subject of parliamentary scrutiny of intelligence, and has been a Fellow of the Fulbright Commission and the U.S. Department of State.

Sweden:

Iain Cameron is a Professor of Public International Law at Uppsala University. He has been a member of the Council of Europe Commission on Democracy through Law since 2005. He has also been a Rapporteur for the journal European Public Law (1995-2009) and Expert in Commission of Inquiry into UN and EU Sanctions. He is the author of several books including *An Introduction to the European Convention on Human Rights* (2011), *International Criminal Law from a Swedish Perspective* (2011), and *National Security and the European Convention on Human Rights* (2000).

Turkey:

Yaman Adkeniz is a Professor of Law at the Human Rights Law Research Center, Faculty of Law, Istanbul Bilgi University. Previously, he was a senior lecturer at the School of Law, University of Leeds. Akdeniz is also the founder and director of Cyber-Rights.Org based in the UK, and the co-founder of BilgiEdinmeHakki.org, a pressure group working in the field of freedom of information law in Turkey. He authored the Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship (January 2010).

United Kingdom:

Adam Tomkins is the John Millar Chair of Public Law at the University of Glasgow. Among his books are two of the bestselling and leading works on British constitutional law: *Public Law* (OUP, 2003) and *British Government and the Constitution* (CUP, 7th ed 2011). His work has been cited in leading House of Lords case law. In 2009, he was appointed a legal adviser to the House of Lords Select Committee on the Constitution. In 2010, he gave expert evidence in a case concerning freedom of information and the constitutional position of the Prince of Wales.