A Balancing Act between Crime Prevention and Privacy Protection

Proposal for a Privacy Protection Guideline on Secret Personal Data Gathering and Transborder Flows of Such Data in the Fight against Terrorism and Serious Crime

Thesis by

Marcel Stüssi MLaw (Lucerne)

First presented to the chair on public law and theory of legislation, deputy vice chancellor
Prof. Dr. iur. Paul Richli - University of Lucerne

Table of Contents

TABLE OF CONTENTS I
TABLE OF INTERNATIONAL LEGAL INSTRUMENTS AND GENERAL COMMENTS III
TABLE OF DOMESTIC LEGISLATION III
TABLE OF CASES VI
TABLE OF NON-AUTHORITATIVE SOURCES VI
LIST OF ABBREVIATIONS IX

PREFACE 1

PART I - GENERAL 4

A. DEFINITIONS 4
B. PURPOSE 4
C. SCOPE 5

PART II - BASIC PROPOSALS OF NATIONAL APPLICATION 6

A. PRIME INDICATIONS 6
Article 1 Indications as to the Grounds, Methods and Control 6
B. APPLICATIONS 6
Article 2 Indication as to Applications 6
Article 3 Record Keeping of Applications 6
C. CATEGORIES 7
Article 4 Categories of Secret Personal Data Gathering 7
D. AUTHORISATIONS 7
Article 5 Indications as to Authorisation 7
Article 6 The Higher Authorising Authority 7
Article 7 The Designated Authorising Authority 7
Article 8 Formalities 8
Article 9 Record Keeping of Authorisations 8
Article 10 Renewal of Authorisations 8
Article 11 Record Keeping of Renewable Authorisations 8
Article 12 Withdrawal of Authorisations 9
Article 13 Record Keeping of Withdrawn Authorisations 9

PART III – BASIC PROPOSALS OF INTERNATIONAL APPLICATION 10

A. PUBLIC AUTHORITY SENDING SECRETLY GATHERED PERSONAL DATA 10
Article 14 Privacy Compliance, Query of the Sender Public Authority 10
Article 15 Exceptional Transfer Due to Substantial Public Interest 10
Article 16 Record Keeping by the Sending Public Authority 10
B. THE PUBLIC AUTHORITY RECEIVING SECRETLY GATHERED PERSONAL DATA 11
Article 17 Privacy Compliance, Query of the Recipient Public Authority 11
Article 18 Exceptional Receipt and Special Personal Data Marking 11
Article 19 Record Keeping by the Recipient Public Authority 11
C. INTERNATIONALLY ACCESSIBLE DATABASE OF SECRETLY GATHERED PERSONAL DATA 12
Article 20 Personal Data Filing 12
D. TRANSBORDER LIBERALISATION OF SECRETLY GATHERED PERSONAL DATA 12
Article 21 Transborder Liberalisation 12

PART IV - PROPOSAL OF INTERNATIONAL AS WELL AS NATIONAL APPLICATION 13

A. REASONABLENESS 13
Article 22 The Test 13

PART V - NATIONAL IMPLEMENTATION 14

A. NATIONAL IMPLEMENTATION 14

PART VI - INTERNATIONAL COOPERATION 15

A. INTERNATIONAL COOPERATION 15

PART VII - EXPLANATORY MEMORANDUM 16

1. INTRODUCTION 16
1.1 Purpose *16*
1.2 Scope *16*
1.3 Legal Disparities *17*
1.3.1 Disparity between South Africa and Australia 18
1.3.2 Disparity between Switzerland and the United Kingdom 18
1.3.3 Disparity between Mexico and the United States of America 19
1.4 State Obligation to fight Terrorism and Serious Crime *20*
1.5 State Duty to Respect Privacy and Individual Liberties *20*
1.6 Need for a Balancing Act *21*
2. BASIC PROPOSAL OF NATIONAL APPLICATION 22
2.1 Prime Indications *22*
2.1.1 Article 1 Indications as to the Grounds, Methods and Control 22
2.2 Applications *23*
2.2.1 Article 2 Indication as to Applications 23
2.2.2 Article 3 Record Keeping of Applications 24
2.3 Categories of Secret Personal Data Gathering *25*
2.3.1 Article 4 Categories of Secret Personal Data Gathering 25
2.4 Authorisation of Secret Personal Data Gathering *28*
2.4.1 Article 5 Indications as to Authorisation 28
2.4.2 Article 6 The Higher Authorising Authority 29
2.4.3 Article 7 The Designated Authorising Authority 30
2.4.4 Article 8 Formalities 30
2.4.5 Article 9 Record Keeping of Authorisations 31
2.4.6 Article 10 Renewal of Authorisations 31
2.4.7 Article 11 Record Keeping of Renewable Authorisations 32
2.4.8 Article 12 Withdrawal of Authorisations 32
2.4.9 Article 13 Record Keeping of Withdrawn Authorisations 32
3. BASIC PROPOSAL OF INTERNATIONAL APPLICATION 32
3.1 Public Authority Sending Secretly Gathered Personal Data *32*
3.1.1 Article 14 Privacy Compliance, Query of the Sender Public Authority 32
3.1.2 Article 15 Exceptional Transfer Due to Substantial Public Interest 33
3.1.3 Article 16 Record Keeping by the Sender Public Authority 33
3.2 The Public Authority Receiving Secretly Gathered Personal Data *34*
3.2.1 Article 17 Privacy Compliance, Query of the Recipient Public Authority 34
3.2.2 Article 18 Exceptional Receipt and Special Personal Data Marking 35
3.2.3 Article 19 Record Keeping by the Recipient Public Authority 36
3.3 Internationally Accessible Database of Secretly Gathered Personal Data *36*
3.3.1 Article 20 Personal Data Filling 36
3.4 Transborder Liberalisation of Secretly Gathered Personal Data *36*
3.4.1 Article 21 Transborder Liberalisation 36
4. BASIC PROPOSAL OF INTERNATIONAL AND NATIONAL APPLICATION 37
4.1 Reasonableness *37*
4.1.1 Article 22 The Test 37
5. NATIONAL IMPLEMENTATION 37
6. INTERNATIONAL COOPERATION 38

PART VIII - CONCLUSION 39

1. CONSIDERATIONS IN THE NARROW SENSE 39
2. CONSIDERATIONS IN THE WIDER SENSE 42

PART IX - SUMMARY 48

PART X - APPENDICES 49

1. TABLE OF PRIME METHODS OF SECRET INFORMATION GATHERING 49
2. TABLE OF MECHANISMS OF CONTROL 50
3. TABLE OF OFFICIAL LEGISLATION SOURCES 51
4. STATEMENT OF INDEPENDENCE AS TO THE COMPOSITION OF THIS PAPER 52

Table of International Legal Instruments and General Comments

A. International Legal Instruments

International Covenant on Civil and Political Rights of 1966
art 2 20
art 6(1) 20
art 17 .... 3, 21, 22, 26, 35
Council Directive (EC) 95/46
art 8(1) 27
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980
para 7 22
para 9 22
para 14 ....16, 35
para 17 36
UN Security Council Resolution 1373 of 2001
para 3(a) 1
UN General Assembly Resolution 60/251 of 2006 40

B. General Comments

UN Human Rights Committee “General Comment 6” of 1982
para 2 20
para 3 20
para 5 20
UN Human Rights Committee “General Comment 16” of 1988
para 3 ....21, 22
para 4 ....21, 24
para 8 .... 21, 22, 26, 27

Table of Domestic Legislation

A. National Legislation of the Commonwealth of Australia

Australian Bill of Rights of 15 November 1985
art 12 18
Surveillance Device Act 2004
s 10 30
s 11 ....50, 29
s 14 ....23, 30
s 14(1) 23, 30, 50
s 14(1)(a) 22
s 14(5) 23
s 15 23
s 17(1)(ix) 29
s 18 ....22, 25, 49
s 19 32
s 20 32
s 28 23
s 29 30
s 30 30
s 31 23

s 31(1) 24
s 33 18
s 49 24

B. National Legislation of the United Mexican States

National Security Act 2005
art 5 22
art 33 23
art 34 20
art 38 24
art 39 ..... 1, 30, 50
art 40 ..... 29, 30
art 45 24
art 49 ..... 23, 30
Political Constitution of the United Mexican States of 1917
art 16 20

C. National Legislation of the Republic of South Africa

Intelligence Services Act 2002
s 11(2) 23, 29, 30, 50
s 11(2)(b) 23
s 11(3)(a) 29
s 11(4) 32
s 39(a) 37
Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002
s 16(2) 24
s 16(2)(c) 24
s 23(8) 30
s 7(1) 18, 23
s 7(1)(a) 23
s 7(1)(a)(i) 22
s 7(1)(a)(ii) 22
s 7(1)(a)(iii) 22
s 7(1)(b) 18
s 7(1)(c) 22, 25, 49

D. National Legislation of the Swiss Confederation

Federal Act about Measures for the Protection of National Security 1997
art 14(1) 18, 22, 23
art 14(2) 22, 25, 49
art 14(2)(a) 18, 19, 50
art 14(2)(b) 18, 19, 50
art 14(2)(c) 18, 19, 50
art 14(2)(d) 18, 19, 50
art 14(2)(e) 18, 19, 50
art 14(2)(f) 18, 19, 50
art 14(2)(g) 18, 19, 50
Federal Constitution of the Swiss Confederation of 1999
art 10 19
art 13 19

E. National Legislation of the United Kingdom of Great Britain and Northern Ireland

Code of Practice, Acquisition and Disclosure of Communications Data 2006
para 2.3 30
para 3.11 30
para 3.22 30
para 3.33 32
para 3.36 32
para 3.42 ..... 23, 30
para 3.43 30
para 3.44 30
para 3.45 30
para 6.19 33
Code of Practice, Covert Surveillance 2006
para 2.4 ..... 1, 30, 50
para 2.5 ..... 1, 30, 50
para 2.6 ..... 1, 30, 50
para 2.7 ..... 1, 30, 50
para 2.8 37
para 2.9 ..... 1, 30, 50
para 2.10 ..... 1, 30, 50
para 4.19 29
para 4.2 29
para 4.9 24
para 5 24
para 5.16 24
para 5.18 24
para 5.3 25
Human Rights Act 1998
schedule 1, art 8(1) 19
Regulation of Investigatory Powers Act 2000
s 6 23
s 7 23
s 28 ..... 22, 25, 29, 49
s 28(1) 19
s 28(3) 30
s 29 ..... 22, 25, 49
s 29(3) 22, 23
s 32(1) 18
s 32 ..... 22, 25, 49
s 32(3)(a) 30
s 32(6) 29
s 33(5) 23
s 34 23

F. National Legislation of the United States of America

Foreign Intelligence Surveillance Act 1978
para 1801(e) 22
para 1801(f) 22, 25, 49
para 1802(a)(1) 30
para 1804(a) 19, 23, 29
para 1804(a)(1) 23
para 1805(a)(1) 29
para 1805(b) 1, 30, 24, 50
para 1805(c) 24
para 1805(f) 24, 30
para 1805(3) 30
para 1811 ..... 19, 20

Table of Cases

A. European Human Rights Reports

B v France (1993) 16 EHRR 1, paras 55-62 27
Buckley v United Kingdom (1996) 23 EHRR 101 26
Dudgeon v United Kingdom (1981) 4 EHRR 149, para 52 27
Gaskin v United Kingdom (1989) 12 EHRR 36 ....25, 27
Gillow v United Kingdom (1986) 11 EHRR 335....26
Murray v United Kingdom (1994) 19 EHRR 193 26
Niemetz v Germany (1992) 16 EHRR 97....26, 27
Z v Finland (1997) 25 EHRR 371 27

B. European Commission of Human Rights Reports

Kanthak v Germany (1988) 58 DR 94, EComm HR 26

Table of Non-Authoritative Sources

A. List of References

The following publications are cited in accordance with “The Oxford Standard for Citation of Legal Authorities”.

Becker Ernest	Dynamik des Todes, Die Überwindung der Todesfurcht, Ursprung der Kultur, Freiburg 1976
Bierbrauer Günter	Interkulturelles Verhandeln, F. Haft v. Schlieffen (Hg.): Handbuch Mediation, München 2002, p 266-288
Bierbrauer Günter	Triebe, Instinkte, Kultur und Todesangst: Osnabrücker Jahrbuch Frieden und Wissenschaft, Göttingen, Universität Osnabrück 2003, p 137-146
Darwin Charles Robert	The Expression of the Emotions in Man and Animals, John Murray, London 1872
Häfelin Ulrich/ Haller Walter	Schweizerisches Bundesstaatsrecht, 5. Auflage: Schulthess Juristische Medien AG, Zürich 2001, para 1650
Hegel Georg Wilhelm Friedrich	Grundlinien der Philosophie des Rechts von 1820, Helmut Reichelt: Ullstein-Buch, Frankfurt am Main 1972
Herskovits Melville Jean	Man and His Works, The Science of Cultural Anthropology, New York 1948

Kant Immanuel	Essay Beantwortung der Frage, Was ist Aufklärung: Berlinische Monatsschrift, Johann Erich Biester und Friedrich Gedike, Berlin 1784
Kelman Herbert	Interactive Problem Solving as a Metaphor for International Conflict Resolutions, Lessons for the Policy Process, Peace and Conflict: Journal of Peace Psychology, 1999, p 201-218
Kölz Alfred/ Häner Isabelle	Nachdenken über den demokratischen Staat und seine Geschichte, Aufsatz von Helen Keller, Antiterrormassnahmen, Verfahrensschutz bei der Sperrung von Banknoten: Schulthess, Zürich 2003, p 299 ff
Montesquieu Charles-Luis de Secondat/ J. V. Prichard (tr)	De L'Esprit des Lois of 1748: G. Bell & Sons, Ltd., London 1914
Müller Georg	Elemente einer Rechtssetzungslehre: Schulthess Juristische Medien AG, Zürich 1999, p 146 ff
Nowak Manfred	M Nowak, U.N. Covenant on Civil and Political Rights, CCPR Commentary, Kehl, Strasbourg, Arlington 1993, p 302 ff
Richli Paul	Interdisziplinäre Daumenregeln für eine faire Rechtsetzung: Helbing & Lichtenhahn Verlag, Basel 2000, p 13 ff
Solomon Sheldon/ Greenberg Jeff/ Pyszczynski T.	A Terror Management Theory of Social Behaviour, The Psychological Functions of Self-Esteem and Cultural Wold Views, Mark P. Zanna (ed.), Advances in Experimental Social Psychology 1991, p 93-159

B. Internet Sources

(Aus) Attorneys General's Office: http://www.nationalsecurity.gov.au.....51
(CH) Legislation Database: http://www.admin.ch/ch/d/sr/sr.html 51
(Mex) UNAM Database: http://info4.juridicas.unam.mx/ijure/fed.....51
(SA) Legislation Database: http://www.info.gov.za/aboutgovt/dept.htm 51
(UK) Home Office: http://security.homeoffice.gov.uk/news-and-publications1 51
(US) Law Revisions Council: http://uscode.house.gov/search/criteria.shtml 51
(CH) Office Féderal de la Statistique, "Infraction Lois" http://www.bfs.admin.ch 44
(Aus) Office of Crime Statistics and Research: http://www.ocsar.sa.gov.au 44
(SA) Cape Gateway: http://www.capegateway.gov.za/eng/pubs/public_info/C/86878/1.....44
(UK) Home Office, Research Development Statistics: http://www.homeoffice.gov.uk 44
(UN) Counter-Terrorism Committee: http://www.un.org/sc/ctc/law.shtml 1, 17, 39, 43
(US) Bureau of Justice Statistics: http://www. albany.edu/sourcebook/pdf/t31062004.pdf 44
Wikipedia, the Free Encyclopaedia: http://en.wikipedia.org/wiki/Main_Page 46

C. Reports

(UK) Nolan Report, Standards in Public Life, Cm 2850-I, 1995, London: HMSO 40
(CH) Prise de position du PFPD concernant l'avant-projet de révision de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure.....29
(UK) Report of the Intelligence Service Commissioner for 2003, HC, 2004-07, 884.....35
(UK) Report of the Interception of Communications Commissioner for 2003, HC, 2004-07, 883.....35
(US) Department of State Publication, Country Report on Terrorism, April 2006, p 287.....43

D. Journalistic Sources

(US) The New York Times, Bush Lets U.S. Spy on Callers Without Courts, 16 December 2005 19

List of Abbreviations

%	percent
approx	approximately
art	article
Aus	Commonwealth of Australia
CH	Confoederatio Helvetica – Swiss Confederation
cl	comparative law
CP-ADCD	Code of Practice, Acquisition and Disclosure of Communications Data 2006 (UK)
CP-CS	Code of Practice, Covert Surveillance 2006 (UK)
EC	European Community
ECHR	European Convention on Human Rights (1950)
EComm HR	European Commission of Human Rights
ECtHR	European Court of Human Rights
Eg	For example
EHRR	European Human Rights Law Reports
EU	European Union
FISA	Foreign Intelligence Surveillance Act 1978 (US)
FPNS	Federal Act about Measures for the Protection of National Security 1997/Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit 1997 (CH)
ICCPR	International Covenant on Civil and Political Rights (1966)
ISA	Intelligence Services Act 2002 (SA)
Mex	United Mexican States
n	number
NSA	National Security Act 2005/Ley de Seguridad Nacional de 2005 (Mex)
OECD	Organisation for Economic Cooperation and Development
para	paragraph
paras	paragraphs
Res	Resolution
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002 (SA)
RIPA	Regulation of Investigatory Powers Act 2000 (UK)
s	section
SA	Republic of South Africa
SDA	Surveillance Device Act 2004 (Aus)
SPDG	Secret Personal Data Gathering
tr	translation
UK	United Kingdom of Great Britain and Northern Ireland
UN	United Nations

UNGA	United Nations General Assembly
UNHRC	United Nations Human Rights Committee
UNSC	United Nations Security Council
US	United States of America

Preface

The guideline proposed in this paper considers privacy protection in two respects. Firstly, the domestic enforcement of the 13 international legal instruments[1] that play an integral part in counter-terrorism measures relies heavily upon the covert acquisition of personal data. And secondly, the State duty to protect the people from truly horrific or gruesome acts of terrorism and serious crime[2] requires that *inter alia* Governments cooperate by exchanging large amounts of secretly gathered personal data across national frontiers, and indeed across continents.[3] Such data flows have greatly increased in recent years and may grow even further at this time of renewed political tension and in the light of the fact that religious and cultural frictions are being exploited for violent ends.

Privacy protection provisions in relation to covert operations or investigations have been introduced, or will be introduced shortly.[4] The Commonwealth of Australia, the United Mexican States, the Republic of South Africa, the United Kingdom of Great Britain and Northern Ireland, and the United States of America have, among other countries, passed legislation.[5] The Swiss Confederation has prepared a draft bill to prevent what are considered to be violations of fundamental human rights, such as the arbitrary and unlawful acquisition of personal data through intrusive surveillance and the interception of communications.[6]

By having regard to the different levels of privacy protection in each country,[7] there is, however, a danger that disparities in national legislation[8] could not only hamper the free flow of personal data across frontiers, but infringe on the privacy rights of the data subjects concerned.

The recommendations set forth in this guideline are an attempt to balance the two basic values against one other: the protection of terrorism and other criminal

---

1 See generally Internationally Applicable Counter-Terrorism Convention and Protocols at UNSC, “Counter-Terrorism Committee” <http://www.un.org/sc/ctc/law.shtml> accessed 13 May 2006

2 See part VII, para 1.4.

3 See UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373, para 3(a).

4 See generally part X, para 2.

5 See generally SDA; NSA; ISA and RICA; CP-ADCD, CP-CS and RIPA; FISA.

6 Swiss draft bill, Bundesamt für Justiz, Vorentwurf zur Revision des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit, Berne 31 January 2006 <http://www.ejpd.admin.ch> accessed 3 May 2006

7 Eg see cl, SDA, s 14(1); NSA, art 39; ISA, s 11(2); CP-CS, para 2.4 to 2.10; FISA para 1805(b).

8 See part VII, para 1.3.

activities on the one side, and the respect for privacy and individual liberties on the other. The proposal recognises that certain country-specific differences to SPDG are indispensable because of varying levels of threat posed to particular State territories. It nevertheless seeks to reduce the need for such differences, by introducing mechanisms of executive control and administrative procedures[9] that can accommodate different approaches to privacy, tailored to national legal and cultural norms, and that will enable global information flow while respecting those norms. Moreover, the guideline endeavours to strengthen the notion of free transborder information flows by calling upon Governments to waive additional restrictions which could obstruct the effective prevention of terrorism and serious crime.

The legal provisions proposed help harmonise national privacy protection laws and, while upholding such human rights, should prevent at the same time interruptions in international flows of secretly gathered personal data. The recommendations can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it. Particular heed has been paid to the freedom of action in view of country-specific incorporations. Domestic and cultural traditions and values must be respected when considering the meaning and scope of human rights.[10]

This paper mirrors a minimum standard for the protection of privacy in the fight against terrorism and serious crime. Its primary focus rests upon the secret acquisition of personal data, and the subsequent personal data sharing process between Governments. It is intended to serve as a basis for discussion only. The guideline is accompanied by an Explanatory Memorandum which provides information on the reasoning underlining the formulation of the recommendations.

---

9 See generally part II to part IV.

10 See part VII, para 2.4.2.

Proposal for a Privacy Protection Guideline on Secret Personal Data Gathering and Transborder Flows of Such Data in the Fight against Terrorism and Serious Crime

States, by having regard to Article 17 of the International Covenant on Civil and Political Rights of 16 December 1966, should recognise

(a) that, although national laws and policies may differ, countries have a common interest in protecting privacy and individual liberties;

(b) that domestic legislation concerning privacy protection and transborder flows of personal data may hinder the flow of such data;

(c) that, the promotion and protection of human rights should be based on the principles of cooperation and genuine dialogue and be aimed at strengthening the capacity of States to comply with their privacy obligations for the benefit of all data subjects; and

(d) that the global security environment is dynamic, and States should continually respond to ensure that the legislative regime is current, comprehensive and appropriate.

Determined to advance the free flow of information between States and to avoid the creation of unjustified obstacles to the prevention of terrorism and serious crime, this guideline proposes

(a) that countries take into account the principles concerning the protection of privacy set forth in this guideline;

(b) that countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of secretly gathered personal data; and

(c) that countries cooperate in the implementation of the guideline.

Part I - General

A. Definitions

(1) For the purposes of this guideline

(a) "personal data" means any information relating to an identified or identifiable individual;

(b) "data subject" means an identified or identifiable individual;

(c) "secret personal data gathering" means any acquisition of personal data that is calculated to ensure that the data subject to an investigation or operation is unaware that it is or may be taking place;

(d) "transborder flows of personal data" means movements of personal data across national borders;

(e) "public authority or public official" means any person certain of whose functions are of a public nature, and a court or tribunal, but does not include Parliament or a person exercising functions in connection with proceedings in Parliament.

B. Purpose

(1) This guideline proposes a framework of laws and procedures to Governments with a view to

(a) achieving acceptance of certain minimum standards of protection of privacy with regard to secret personal data gathering and the transferring of such data to foreign recipient Governments;

(b) reducing differences between relevant domestic laws and practices to a minimum;

(c) ensuring that in protecting personal data they take into consideration the interests of other countries and the need to avoid undue interference with flows of personal data between countries in the fight against terrorism and serious crime; and

(d) eliminating, as far as possible, reasons which might prompt governments to restrict transborder flows of such data because of the possible risks associated with the flows.

C. Scope

(1) This guideline should apply to systematic secret personal data gathering whether outside or inside a State's territory

(a) for a preventive purpose in the interests of national security, public safety, or for the prevention of disorder and crime;

(b) in the public sectors which, because of the manner in which personal data is gathered, or because of its nature or the context in which it is used, poses a danger to privacy and individual liberties;

(c) in times of peace, international and non-international armed conflict; and

(d) be regarded as a minimum standard which is capable of being supplemented by additional measures.

Part II - Basic Proposals of National Application

A. Prime Indications

Article 1 Indications as to the Grounds, Methods and Control

(1) The law should indicate

(a) the grounds for secret personal data gathering;

(b) the methods which may be applied; and

(c) the public authority having power or control over the exercise of secret personal data gathering.

B. Applications

Article 2 Indication as to Applications

(1) The law should indicate

(a) the authority having the power to apply for secret personal data gathering;

(b) that an application for secret personal data gathering must be made in relation to the grounds indicated by the law; and

(c) the formalities required for an application.

Article 3 Record Keeping of Applications

(1) A record of all applications for secret personal data gathering should be kept and contain the following information:

(a) the public authority applying;

(b) the grounds for the application;

(c) the category of application; and

(d) why the public authority believes that secret personal data gathering is, under the particular circumstances of the case, reasonable.

(2) Such record should be kept regardless of whether the application was made in writing, electronically, or orally.

C. Categories

Article 4 Categories of Secret Personal Data Gathering

(1) Category I Secret Personal Data Gathering may be exercised by

(a) intrusive surveillance and interception; or

(b) the acquisition of intimate personal data.

(2) Category II Secret Personal Data Gathering may be exercised by

(a) non-intrusive surveillance and non-intrusive interception that is not covered under paragraph *(3)* of this Article; or

(b) the acquisition of non-intimate personal data that is not covered under paragraph *(3)* of this Article.

(3) Category III Secret Personal Data Gathering may be exercised by the acquisition of open source personal data and does not require an authorisation.

D. Authorisations

Article 5 Indications as to Authorisation

(1) The law should indicate

(a) the public authority which has the power to authorise secret personal data gathering;

(b) the maximum duration for any authorisation; and

(c) that the public authority must authorise secret personal data gathering for a reasonable period of time only.

Article 6 The Higher Authorising Authority

(1) The Higher Authorising Authority should reasonably consider and may authorise

(a) Category I Secret Personal Data Gathering; or

(b) applications made in relation to grounds expressly indicated in the law.

Article 7 The Designated Authorising Authority

(1) The Designated Authorising Authority should reasonably consider and may authorise

(a) Category II Secret Personal Data Gathering; or

(b) applications made in relation to grounds expressly indicated in the law.

Article 8 Formalities

(1) Authorisations may be granted in writing, electronically, or orally.

(2) Oral authorisation should only be given in exceptional circumstances.

Article 9 Record Keeping of Authorisations

(1) A record of all authorisations for secret personal data gathering should be kept and contain the following information:

(a) the public authority applying;

(b) the grounds for the application;

(c) the category of application;

(d) the reason why the applying public authority believes it to be reasonable;

(e) the reason why the authorising public authority agrees or disagrees that it is reasonable;

(f) whether a particular application was approved or disapproved;

(g) by which public authority it was approved or disapproved; and

(h) the date and time the decision for approval or disapproval was taken.

(2) Such record should be kept regardless of whether authorisation was made in writing, electronically, or orally.

Article 10 Renewal of Authorisations

(1) The law should indicate that

(a) an authorisation may be renewed where appropriate;

(b) the time must be reasonable for any renewable authorisation; and

(c) any application for renewal must be made in writing, or electronically.

Article 11 Record Keeping of Renewable Authorisations

(1) A record of all renewable authorisations should be kept and contain the following information:

(a) the public authority applying for a renewal;

(b) the grounds for the application for a renewal;

(c) why the applying public authority believes secret personal data gathering to be reasonable;

(d) why the authorising public authority agrees or disagrees that secret personal data gathering is reasonable;

(e) whether the particular application for renewal was approved or disapproved;

(f) by which public authority secret personal data gathering was approved or disapproved;

(g) the date and time the renewal was approved or disapproved.

Article 12 Withdrawal of Authorisations

(1) Where an authorisation becomes unnecessary, unsuitable, or is no longer proportionate to what is sought to be achieved, that authorisation should be withdrawn by the respective authorising public authority.

Article 13 Record Keeping of Withdrawn Authorisations

(1) A record should be kept which indicates

(a) the reason for withdrawal;

(b) the date and time when a particular authorisation was withdrawn;

(c) the authorising public authority which withdrew the authorisation.

Part III – Basic Proposals of International Application

A. Public Authority Sending Secretly Gathered Personal Data

Article 14 Privacy Compliance, Query of the Sender Public Authority

(1) Where a public authority is about to send secretly gathered personal data across its borders to a foreign recipient public authority, it should consider whether the sending of that data is reasonable in the circumstances of the case, and whether the data will be adequately protect by the foreign recipient public authority.

Article 15 Exceptional Transfer Due to Substantial Public Interest

(1) Where the public authority sending secretly gathered personal data reasonably considers that there is no adequate protection by the foreign recipient public authority, but the transfer of the data is of substantial public interest, that data may still be transferred.

Article 16 Record Keeping by the Sending Public Authority

(1) A record of secretly gathered personal data that is transferred to a foreign recipient public authority should be kept and contain the following information:

(a) a description of the content of the secretly gathered personal data;

(b) the name of the public authority sending the personal data;

(c) the name of the public authority receiving the personal data;

(d) the date and time when the personal data was sent and received;

(e) whether the public authority sending the secretly gathered personal data considers that the transfer is reasonable under the specific circumstances of the case;

(f) whether the public authority sending the secretly gathered personal data considers that the data is adequately protected by the foreign recipient public authority; and

(g) the reasons why the data was still transferred although the public authority sending the personal data considered that the data was not adequately protected by the foreign recipient public authority.

B. The Public Authority Receiving Secretly Gathered Personal Data

Article 17 Privacy Compliance, Query of the Recipient Public Authority

(1) The public authority receiving secretly gathered personal data should inquire whether the public authority sending the data either complies with the guidelines set forth in this framework, or has ratified similar provisions which protect the right to privacy equally. It should also consider whether receiving the data is reasonable under the particular circumstances of the case.

Article 18 Exceptional Receipt and Special Personal Data Marking

(1) Where the public authority sending the secretly gathered personal data does not comply with the guidelines under this framework and has not ratified similar provisions which would protect the right to privacy equally, or the public authority in question has not gathered but merely transferred the secretly gathered personal data from one foreign public authority to another, that data may still be received in a case of substantial public interest.

(2) Personal data which is gathered under the procedure covered in paragraph *(1)* of this Article should be especially marked.

Article 19 Record Keeping by the Recipient Public Authority

(1) A record of secretly gathered personal data that is received from a foreign public authority should be kept and contain the following information:

(a) a description of the content of the secretly gathered personal data;

(b) the name of the public authority sending the personal data;

(c) the name of the public authority receiving the personal data;

(d) the date and time when the personal data was received;

(e) an explanation about the reason for receiving the secretly gathered personal data;

(f) whether the procedures of the public authority sending the personal data comply with this guideline, or the State in question has ratified similar provisions which protect the right to privacy equally; and

(g) the reason why the personal data was still transferred despite the fact that the public authority sending the personal data did not comply with this guideline, or has not ratified similar provisions which protect the right to privacy equally.

C. Internationally Accessible Database of Secretly Gathered Personal Data

Article 20 Personal Data Filing

(1) Personal data which is gathered secretly should not be filed in an internationally accessible database unless the public authority which gathered the personal data complied with the Proposals of National Application set forth in this guideline, or the State in question has ratified similar provisions which protect the right to privacy equally.

D. Transborder Liberalisation of Secretly Gathered Personal Data

Article 21 Transborder Liberalisation

(1) Restrictions on the international flow of secretly gathered personal data, other than the ones covered by this guideline, should be waived. States have a common interest to intensify and accelerate the exchange of secretly gathered personal data and to cooperate to prevent and suppress terrorism and serious crime.

Part IV - Proposal of International as well as National Application

A. Reasonableness

Article 22 The Test

(1) A public authority exercises its powers reasonably, if it believes that they are

(a) necessary to achieve the relevant purpose;

(b) suited to achieve the purpose intended; and

(c) proportionate to the importance of the particular objective to be achieved.

(2) A public authority, or individual public official, that acts contrary to paragraph *(1)* should be held accountable under this Article.

Part V - National Implementation

A. National Implementation

(1) In implementing domestically the proposals set forth in the guideline, States should establish legal, administrative or other procedures or institutions for the protection of privacy in respect of secret personal data gathering. States should in particular endeavour to

(a) adopt appropriate domestic legislation; and

(b) ensure that there is no unfair discrimination against data subjects.

Part VI - International Cooperation

A. International Cooperation

(1) States should find in concert an adequate categorisation for secret personal data gathering.

(2) States should make known to other countries details of the observance of the principles set for in these guidelines.

(3) States should also ensure that procedures for transborder flows of personal data and for the protection of privacy are simple and compatible.

(4) States should establish procedures to facilitate

(a) secretly gathered personal data exchange; and

(b) mutual assistance in pre-emptive investigative matters.

Part VII - Explanatory Memorandum

1. Introduction

Prior to explaining the reasoning behind the individual principles set forth in this guideline, this explanatory memorandum provides information on the guideline's purpose and scope, and highlights three specific legal disparities in domestic legislation with regard to SPDG. Moreover, the memorandum takes a brief look at one of the most important aspects of the State's obligation to fight terrorism and serious crime, and then continues by pointing out the need to balance such duties against the general requirement to have respect for privacy and individual liberties.

1.1 Purpose

The paramount purpose of this guideline is to propose a minimum standard of protection of privacy in view of SPDG in the fight against terrorism and serious crime. The guideline recognises that some aspects of the disparities in domestic laws are incommensurable. The guideline nevertheless endeavours not only to reduce differences between relevant national laws and practices to a minimum, but also to eliminate, as far as possible, reasons which might prompt governments to restrict transborder flows of such data.[11]

1.2 Scope

This guideline applies to systematic SPDG whether outside or inside a country's territory. Non-systematic and non-automatic SPDG forms part of the duties of many law enforcement officers and other public authorities. It is thus not regulated under this guideline. For example, police officers will be on patrol to prevent and detect crime, maintain public safety and prevent disorder through observing the public. Such observations do not involve systematic SPDG and are not covered under this framework. Non-systematic SPDG is also used when it comes to technical systems that filter personal information from the internet, other wireless communications or satellite images without systematically investigating the personal data of a specific

[11] Eg because of the possible risks associated with these flows. See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), part two, para 14.

individual. Such non-systematic monitoring does not involve systematic SPDG, and is thus not covered under this guideline.

(2)(a) "For a preventive purpose" means that personal data is gathered secretly with a view to preventing, for instance, a terror attack or to detect and prevent other serious crimes before perpetrators can commit them. SPDG covered under this guideline may thus detect what would be considered inchoate crimes such as attempts, conspiracies or incitements before the actual *actus reus* were carried out.[12]

(2)(b) "In the public sectors" means executive institutions or institutions controlled by the executive of a country.

(2)(c) This guideline should not be restricted to apply to times of peace only, as especially during times of international or non-international armed conflicts privacy and individual liberties are endangered. The recommendations are constructed in a manner that SPDG can be carried out expeditiously and devoid of unnecessary bureaucracy.[13] States should therefore not derogate from the basic principles proposed as long as administrative procedures can be upheld and are run and controlled by the ruling Government.

(2)(d) This guideline provides guidance on procedures and laws that regulate SPDG. It is thought to be a minimum standard and should not hamper governments in taking additional steps to protect the right to privacy and individual liberties.

1.3 Legal Disparities

The highlighting of three specific disparities in national laws should not be interpreted to mean that, through the incorporation of this guideline, they can be brought perfectly into line with each other. As stated in the Preface of this paper, the levels of threat posed to particular State territories vary greatly and so must the mechanisms of control. The reasons why they are still stated are twofold. Firstly, they are extreme differences in national laws which infringe constitutional principles if exercised on a third country's territory. Secondly, and more importantly, the pointing out of the legal reality as it stands today should encourage States to discuss the issue on an international level. The quality of secretly gathered personal data affects any

---

[12] States are required to introduce additional *acti rei* and *mentes reae* to combat terrorism and serious crime into their domestic legal system. See generally Internationally Applicable Counter-Terrorism Convention and Protocols at UNSC, "Counter-Terrorism Committee" <http://www.un.org/sc/ctc/law.shtml> accessed 13 May 2006

[13] See part VII, para 2.4.4.

Government relying on that data, and the degree of privacy protection affects any citizen relying on that Government.

1.3.1 Disparity between South Africa and Australia

Section 7(1) of South African RICA reads:

> […] any law enforcement officer may, if he or she is satisfied that there are reasonable grounds to believe that a party to the communication may cause the infliction of serious bodily harm to another person, intercept any communication or may orally request a telecommunication service provider to route duplicate signals of indirect communications specified in that request to the interception centre designated therein.

The law enforcement officer must be of the opinion that because of the urgency of the need to intercept the communication, it is not reasonably practicable, either orally or in written terms, to make an application for authorisation to a designated judge.[14] However, in Australian law there is no legal principle which would provide a basis for such exceptional interceptions devoid of any mechanism of control. Under Section 33 of the Australian SDA, a law enforcement officer must in any event apply for approval of an emergency authorisation to an eligible judge. *Ergo* any secret interception of personal data as described under Section 7(1) of RICA would breach Australian constitutional laws.[15]

1.3.2 Disparity between Switzerland and the United Kingdom

Swiss security services may, under Article 14(1) of FPNS, gather personal information about a data subject who does not know that this information will eventually reach the Government. There are clear limits to the exercise of such discretion.[16] Swiss public authorities have no legal power to gather personal data secretly when it would require that law enforcement officers intruded into a home.[17] In the UK, however, Part II of RIPA gives the Secretary of State and senior authorising officers the power to grant authorisations for the carrying out of intrusive surveillance such as eavesdropping in a home.[18]

---

14 See RICA, s 7(1)(b).

15 See the right to protection from arbitrary interference in the Australian Bill of Rights of 15 November 1985, art 12.

16 See FPNS, art 14(2)(a)-(g).

17 Ibid.

18 See RIPA, s 32(1).

Provided that SPDG were undertaken by intrusive covert investigations on Swiss territory, such exercise of executive powers would infringe Article 10(2) and 13 of the Federal Constitution of the Swiss Confederation.[19]

A similar constitutional problem would arise under the laws of the United Kingdom. According to the Swiss FPNS, personal data can *inter alia* be gathered by observing activities taking place in public and generally accessible places.[20] Swiss laws do not require any authorisation for this kind of SPDG.[21]

In the UK, however, it is the designated person who must grant authorisation for the carrying out of that kind of surveillance.[22] Any SPDG without an authorisation would in the territory of the United Kingdom be regarded as *ultra vires* and unconstitutional.[23]

1.3.3 Disparity between Mexico and the United States of America

Paragraph 1811 of FISA reads:

> Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.

According to the New York Times such a classified presidential order was signed in 2002.[24] President George W. Bush secretly authorized the National Security Agency to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying.[25]

---

19 See the right to personal freedom and the right to privacy under art 10(2) and art 13 of the Federal Constitution of the Swiss Confederation of 18 April 1999 (as amended until 15 October 2002). It should, however, be noted that if the draft bill issued by the Swiss Ministry of Justice and Police were adopted, executive powers would be widened and include covert operations and investigations in a home. See n 6 above.

20 See FPNS, art 14(2)(f).

21 This disparity in the law would not be brought into line even when the proposed Swiss draft bill becomes adopted. See generally n 6 above.

22 See RIPA, s 28(1) as compared and contrasted with FPNS, art 14(2)(f).

23 See right to respect for private and family life under the Human Rights Act of 9 November 1998, schedule 1, art 8(1).

24 See generally J Risen and E Lichtblau, “Bush Lets U.S. Spy on Callers Without Courts”: *The New York Times*, (New York 16 December 2005).

25 See FISA, para 1804(a).

Although Article 32 of the Mexican NSA provides law enforcement officers with the powers to secretly gather personal data in such manner as they please, Articles 34 and 49 of the same Act state that any time SPDG is exercised, a judicial authorisation is mandatory. Interceptions of communications justified under Paragraph 1811 of FISA would, on Mexican soil, infringe the individual guarantee under Article 16 of the Political Constitution of the United Mexican States of 1917.

1.4 State Obligation to fight Terrorism and Serious Crime

Article 2 of CCPR states that each party to the Covenant undertakes to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the Covenant.

The words “undertake to ensure” not only impose negative obligations in the sense that the State is required to abstain from interfering with a specific human right, but also implies a positive obligation to intervene in the relationship between individuals in order to prevent “private” violations of rights protected under the Covenant.[26]

Article 6(1) of the 1966 Covenant (CCPR) reads:

> Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life.

In its general comment, the UNHRC considered that Governments have the supreme duty to prevent acts of mass violence causing arbitrary loss of life.[27] The expression “inherent right to life” requires that public authorities adopt positive measures for the protection of the right guaranteed under Article 6(1).[28] The effective exercise of covert operations and investigations which have as their objective the disruption of terror plots, prevention of terror attacks and other serious crimes can be regarded as preventive positive measures required under Article 6(1) of the Covenant.

1.5 State Duty to Respect Privacy and Individual Liberties

However, crime and terror prevention may be difficult as perpetrators operate covertly, using clandestine methods to communicate and shield their activities. Governments are required to gather personal data in a manner calculated to ensure

---

[26] The Committee considers that States parties should take measures not only to prevent and punish deprivation of life by criminal acts, but also to prevent arbitrary killing by their own security forces. See UNHRC “General Comment 6” (30 April 1982), para 3.

[27] Ibid paras 2 and 3.

[28] Ibid para 5.

that the individuals subject to the investigation or operation are unaware that it is or may be taking place. Such measures may create a risk of unjustified intrusion into the privacy of persons who are subject to SPDG, and those who are not even directly subject to it. The right to privacy and individual liberties may also be adversely affected where the executive power in question is simply misused.

Article 17(1) and (2) of the CCPR reads:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> Everyone has the right to the protection of the law against such interference or attacks.

The right to privacy under Article 17 (1) of the Covenant (CCPR) is not absolute.[29] State interference may be legitimate where it is envisaged by the law,[30] predictable[31] and reasonable in the circumstances of the particular case.[32]

1.6 Need for a Balancing Act

Striking a reasonable balance between the right to privacy and individual liberties on the one side,[33] and the necessity of interference by public authorities in the interest of, for instance, national security, public safety, and the prevention of crime and disorder on the other,[34] is a critical mission. In Part I to IV, the guideline introduced the principles necessary for the reasonable equilibration of these competing values, and paragraphs 2 to 4 below explain the proposals in more detail.

It should be noted that the proposals made in Part II of the guideline mainly represent a careful selection and reformulation of the most balanced provisions that were implemented by responsible Governments in recent years. Thus, while Part II is based on comparative legal research, Part III focuses on the transborder flow of secretly gathered personal data which has not, or to little extent, been covered by domestic law to date.

---

29 The term “unlawful” means that no interference can take place except in cases envisaged by the law. See UNHRC “General Comment 16” (8 April 1988), para 3.

30 Ibid paras 3 and 10.

31 The law must specify in detail the precise circumstances in which such interference may be permitted. Ibid para 8.

32 Ibid para 4.

33 See generally International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 17.

34 Ibid art 6.

2. Basic Proposal of National Application

2.1 Prime Indications

2.1.1 Article 1 Indications as to the Grounds, Methods and Control

This proposal should ensure that Governments investigate only genuine threats in connection with one or more grounds indicated by law.[35] That law should specify the circumstances in which an interference with Article 17 of the CCPR may be permitted.[36] By having regard to implementation practices of responsible Governments, this includes *inter alia* the indication of the grounds for interference, as well as a specification of the techniques[37] that may be applied. The express naming of the public authority or authorities that have the power to control or exercise the secret acquisition of personal data has as its objective the restriction on government discretions and ultimately the prevention of unlawful and arbitrary interference.[38]

(1)(a) Law, as a system of rules which a particular country recognizes to regulate the actions of its members, should point out the factors forming a basis for SPDG.[39] Such factors or grounds could, for instance, be the interest of national security; the purpose of preventing or detecting crime or of preventing disorder; the interest of economic wellbeing; the interest of public safety, and so forth.[40]

(1)(b) The law should indicate the procedure for accomplishing secret personal data gathering. This includes the pointing out of techniques used to gather personal data secretly. Individuals who pose a threat to national security and public safety will do the utmost not to be detected by investigators. Thus, in order that the techniques for SPDG do not provide important strategic clues how a Government goes about preventing and detecting crime, such indications should be kept very general.[41]

---

35 See UNHRC "General Comment 16" (8 April 1988), para 3; see also OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), part two, para 7.

36 See UNHRC "General Comment 16" (8 April 1988), para 8.

37 Ibid para 3.

38 It is also indispensable to have information on the authorities which are entitled to exercise control over such interference with strict regard for the law. See UNHRC "General Comment 16" (8 April 1988), para 6.

39 Ibid para 8; see also OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), part two, para 9.

40 Eg see cl, SDA, s 14(1)(a); NSA, art 5; RICA, s 7(1)(a)(i) to (iii); FPNS, art 14(1); RIPA, s 29(3); FISA, para 1802 (a) in correlation to para 1801(e).

41 Eg see cl, SDA, s 18; NSA, art 34; RICA, s 7(1)(c); FPNS, art 14(2); RIPA, s 28, 29, and 32; FISA, para 1801(f).

(1)(c) Moreover, the law should indicate the public official or public authority having the power to exercise SPDG. The making known of the authority that may gather personal data secretly should also be kept in very general terms.[42]

2.2 Applications

2.2.1 Article 2 Indication as to Applications

In view of the categorisation made under Article 4 and read in correlation to Article 6 and 7 of the guideline, the exercise of SPDG may require the authorisation of an authorising authority.

(1)(a) Domestic laws should point out the public authority having the power to apply for SPDG.[43] The public authority applying should, before making an application, reasonably consider under which category the secret personal data acquisition will fall. The list of authority or authorities should be drawn up in an exhaustive manner.[44]

(1)(b) The law should also indicate that applications may only be made in relation to the factors forming a basis for SPDG, and which are pointed out by national law.[45]

(1)(c) Moreover, the law should clearly explain the formalities required for an application. This includes the indication of the circumstances under which an authorisation is bound to specific formalities.[46] Comparative legal research of the laws of several countries has shown that applications may be made in writing, electronically, or even orally.[47]

Oral applications, however, should only be made in exceptional circumstances where a reasonable authority believes that there is an immediate threat to life such as that a person's life might be endangered if the application procedure were undertaken in writing or electronically from the outset. After the period of urgency, the normal written process should be completed. The applying authority should in any case complete a retrospective application which includes an explanation of why the urgent process was undertaken.[48]

---

42 Eg see cl, SDA, s 14(1); NSA, art 33; RICA, s 7(1); FPNS, art 14(1); RIPA, s 33(5); FISA, para 1804(a)(1).

43 See UNHRC "General Comment 16" (8 April 1988), para 6.

44 Eg see cl, SDA, s 14; ISA, s 11(2)(b); FPNS, art 14(1); RIPA, s 6; FISA, para 1804(a).

45 Eg see cl, SDA, s 14(1); ISA, s 11(2)(b); FPNS, art 14(1); RIPA, s 29(3); FISA, para 1804(a).

46 Eg see cl, SDA, s 14(5) and s 15; NSA, art 49; ISA, s 11(2); RIPA, s 7; FISA, para 1804(a).

47 Eg see cl, SDA, s 28; RICA, s 7(1)(a); RIPA, s 34.

48 Eg see cl, SDA, s 31; NSA, art 49; CP-ADCD, para 3.42.

2.2.2 Article 3 Record Keeping of Applications

There should be a mechanism of control which prevents unlawful and arbitrary SPDG before it can be carried out by public authorities,[49] and a mechanism of oversight[50] which detects arbitrary and unlawful SPDG once it has been conducted. In order to make a public authority accountable for the carrying out of its powers, or omissions to act, evidence is required. Record keeping is necessary in view of the mechanism of oversight. The general objective is to reduce unlawful interference with the right to privacy to a minimum. However, such record keeping is not only a valuable source of information by means of oversight, but in respect of evidence brought in legal proceedings against dangerous perpetrators on a later date.

(1)(a) to (c) Such indication is necessary in order to make out the authority, the reason, and the category of SPDG. Pointing out the category under which an application was made provides evidence of whether a particular authorisation was requested from the appropriate authority.[51]

(1)(d) The record should contain full particulars of all the facts and circumstances alleged in support of the application. The expression “arbitrary interference” as used in article 17(1) of CCPR can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances.[52] This means equally that the applying public authority should, before making an application, be obliged to reasonably consider under which categorisation the imminent secret personal data gathering will fall.[53]

(2) Records should be kept regardless of whether a specific application was made in writing, electronically, or orally. It should be stressed that this recommendation is indispensable even when the application was made orally.[54]

---

49 As covered under Part II.

50 Such oversight must be understood as a kind of additional audit exercised by a special Committee composed of members of Parliament or members of the Judiciary. There are no recommendations as to mechanisms of oversight in this guideline but the keeping of records is directly linked to it in the sense that without the compilation of evidence there could be no oversight.

51 Eg see cl, SDA, s 49; NSA, art 38; RICA, s 16(2); CP-CS, para 5.16; FISA, para 1805(c).

52 See UNHRC “General Comment 16” (8 April 1988), para 4; part IV, chap A., art 22 and part VII, para 4.1.1; see also cl, CP-CS, para 5.16; FISA, para 1805(b).

53 Eg see cl, NSA, art 38; RICA, s 16(2)(c); CP-CS, para 4.9.

54 Eg see cl, SDA, s 31(1); NSA, art 45; CP-CS, para 5.18; FISA, para 1805(f).

2.3 Categories of Secret Personal Data Gathering

2.3.1 Article 4 Categories of Secret Personal Data Gathering

The comparative legal research which was conducted for the development of this guideline revealed that the domestic legislation of the States vetted require authorisations in respect of the methods of SPDG.[55]

This categorisation concept does, however, contrary to established international human rights interpretations, give no consideration to the type of data to be gathered.[56] So, for instance, a human intelligence source may provide on request information about highly personal aspects of an individual's childhood, development and history related to his or her private life. Such data is regarded as intimate[57] and should deserve the highest form of protection.

Moreover, where for instance under English law[58] a surveillance device is not present on a residential premises or in a private vehicle, SPDG is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. However, by contemplating the fact that technical attainments are fast paced and the quality of the data gathered increases specifically in relation to capturing sound,[59] the conventional categorisation applied by the States vetted becomes more and more questionable.

The categorisation proposed in this paper addresses these and other issues by taking reference from comments made by the UN Human Rights Committee, European human rights case law, and EC Directive 95/46.

A public authority wishing to exercise SPDG would have to ask itself two specific questions in order to evaluate the adequate category of SPDG. The public authority concerned needs to consider whether it reasonably seeks intimate personal data and/or will apply intrusive means for SPDG; or whether it will conduct non-intrusive SPDG and/or reasonably seeks to acquire non-intimate personal data. Provided that both these questions can be answered in the negative, the SPDG to be carried out is

---

55 Eg see cl, SDA, s 18; NSA, art 34; RICA, s 7(1)(c); FPNS, art 14(2); RIPA, s 28, 29, and 32; FISA, para 1801(f).

56 See n 70 to 74 below.

57 *Gaskin v United Kingdom* (1989) 12 EHRR 36.

58 See CP-CS, para 5.3.

59 But not to the extent that it can be said to be of the same quality as might be expected to be obtained from a device actually present on the particular premises or vehicle.

open source. In other words, the public authority must thereby not only think about the type of data to be gathered, but find out specific information about the use of a particular premises or private vehicle prior to collecting personal data secretly.

The following categories should be understood as a recommendation for two reasons. Firstly, the paper refers *inter alia* to various sources of international law which have no global adherence, and secondly, the objective of this guideline is to encourage discussions, thereby keeping the privacy environment dynamic in the sense that governments continually respond to ensure that the legislative regime is current, comprehensive and appropriate. May it thus just be read, discussed and commented on.

Category I

(a) Intrusive surveillance and interception:

Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication such e-mail messages, wire-tapping and recording of conversations, can be regarded as intrusive if conducted in a "home" or sent to or received from a "home".[60]

The term "home", as used in Article 17 of CCPR, is to be understood to indicate the place where a person resides or carries out his usual occupation.[61] The term "home" means any kind of premises irrespective of specific property rights, and it includes also business premises of professional persons.[62]

The ECtHR has given the term "home" a broad interpretation[63] that is very similar to Article 17 interpretations of CCPR. In general, the term is taken to mean the place where a person lives on a settled basis.[64] "Home" might also include a caravan site[65] a holiday home or camper van,[66] or a place of intended, rather than actual, residence.[67] The "home" of a professional person also includes his business

---

60 See UNHRC "General Comment 16" (8 April 1988), para 8.

61 Ibid para 5.

62 See M Nowak, *U.N. Covenant on Civil and Political Rights, CCPR Commentary* (Kehl/Strasbourg/Arlington 1993), p 302 ff.

63 *Niemetz v Germany* (1992) 16 EHRR 97.

64 *Murray v United Kingdom* (1994) 19 EHRR 193.

65 *Buckley v United Kingdom* (1996) 23 EHRR 101.

66 *Kanthak v Germany* (1988) 58 DR 94, EComm HR.

67 *Gillow v United Kingdom* (1986) 11 EHRR 335.

premises.[68] Premises used wholly for work purposes, however, should not be protected under the right to respect for one's home.[69]

(b) Intimate personal data

At the heart of private life is the capacity of the individual to formulate a perception of oneself and to choose one's personal identity. Any data that can be attributed to this concept is intimate. In addition, personal data about the manner in which an individual presents him or herself to the State and to others is intimate.[70] Intimate data includes also information regarding medical data;[71] data on highly personal aspects of a person's childhood, development and history related to his or her private life;[72] data that encompasses the choice about personal relationships with others, in particular, social and sexual activities;[73] as well as data revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, and trade union memberships.[74]

Category II

It includes any type of surveillance and interception, or data type not covered by Categories I and III of this guideline. Examples of these would be the following:

(a) Surveillance and interception not covered under Categories I and III.

This head covers surveillance and interceptions not conducted in a "home" or sent to or received from a "home".[75] This would include surveillance and interceptions with regard to accessible and public places, or a premises and vehicle used wholly for work purposes. Category II would not include non-systematic surveillance and interception as covered under Category III of this Guideline.

(b) Personal data not covered under Categories I and III.

Although this head refers to any information relating to an identified or identifiable individual, it does not cover the type of data as understood in Categories I and III. An example of such data would be data about a particular bank account holder,

---

68 *Niemetz v Germany* (1992) 16 EHRR 97.

69 Ibid.

70 See *B v France* (1993) 16 EHRR 1, paras 55-62.

71 *Z v Finland* (1997) 25 EHRR 371.

72 *Gaskin v United Kingdom* (1989) 12 EHRR 36.

73 See *Dudgeon v United Kingdom* (1981) 4 EHRR 149, para 52.

74 See Council Directive (EC) 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281, art 8(1).

75 See UNHRC "General Comment 16" (8 April 1988), para 8.

information as to tax payments, or records as to the profession and address of a person.

Category III

This category covers open source secret personal data gathering. Such data may be revealed on the internet, press or any other information source accessible by the public at large.

It covers also information gathered by general observation which forms part of the duties of many law enforcement officers and other public authorities. For example, police officers will be on patrol to prevent and detect crime, maintain public safety and prevent disorder; or trading standards or customs and excise officers might covertly observe and then visit a shop as part of their enforcement function to verify the supply or level of supply of goods or services that may be liable to a restriction or tax.

Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

Open source personal data covers also where members of the public volunteer information to the police or other authorities, as part of their normal civil duties, or contact numbers set up to receive information such as a special Anti-Terrorist Hotline.

Category III open source personal data gathering should not require an authorisation to be issued by a public authority.[76] A public official exercising Category III SPDG should still keep in mind whether the acquisition of the data is suitable, necessary and proportionate in the particular circumstances of the case.

2.4 Authorisation of Secret Personal Data Gathering

2.4.1 Article 5 Indications as to Authorisation

Authorisations for SPDG should be made in respect of the categorisation set forth in Article 4 of this guideline. This means that Category I SPDG should be authorised by a public authority higher up on the ladder of administrative hierarchy than a public authority that may authorise Category II SPDG. In the guideline this differentiation is

[76] Unlike the authorisations required under part II, chap D., art 6 and 7.

made by using the terms “Higher Authorising Authority” and “Designated Authorising Authority”. The empowerment of the particular public authority to authorise interference with the right to privacy should, however, be reserved to the respective States.[77]

(1)(a) The law of a particular country should point out the public official or public authority having the power to authorise SPDG.[78] The list of such an authority or authorities should be drawn up in an exhaustive manner.

(1)(b) The duration of any authorisation should be limited to a maximum period of time.[79]

(1)(c) The authorising authority should specify the shortest period in which the objective for which the personal data is sought can be achieved. To do otherwise will impact on the proportionality of the authorisation and impose an unnecessary burden upon the authority conducting SPDG.[80]

2.4.2 Article 6 The Higher Authorising Authority

The Higher Authorising Authority is part of the doctrine of checks and balances known to every modern democracy. It should be each State on its own that decides the primary function[81] and composition of such authority. In Australia and the United Kingdom it is a Minister or Director of the Security Services who authorises intrusive SPDG.[82] In the United States of America a special tribunal decides about such SPDG authorisations.[83] And in South Africa and Mexico there is a designated judge that exercises this authority.[84]

(1)(a) The Higher Authorising Authority may authorise Category I SPDG. It is the reasonableness test which should be applied in order to reveal whether SPDG is

---

77 For an example of a current debate about the creation of an authorising authority see the commentary issued by the Swiss Federal Information Commissioner regarding the imminent National Security Law Reform. See generally Préposé Fédéral à la Protéction des Données, Prise de position du PFPD concernant l’avant-projet de révision de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI), Berne 17 February 2006 <http://www.edsb.ch/f/aktuell/index.htm> assecced 17 May 2006

78 Eg see cl, SDA, s 11; NSA, art 34; ISA, s 11(2); RIPA, s 28, 29, 32; FISA, para 1805(a)(1).

79 Eg see cl, SDA, s 17(1)(ix); NSA, art 40; ISA, s 11(3)(a); CP-CS, para 4.19.

80 Eg see cl, CP-CS, para 4.2.

81 The particular State should decide whether the authority in question should act on behalf of the executive, judiciary or the legislature.

82 Eg see cl, SDA, s 11; RIPA, s 32(6).

83 Eg see cl, FISA, para 1804(a); however, in some circumstances electronic surveillance may also be conducted without a court order, see FISA, para 1802.

84 Eg see cl, NSA, art 34; ISA, s 11(2).

suitable, necessary and proportionate in the particular circumstances of the case.[85] The authority will be able to exercise its responsible function adequately if it has not only a thorough knowledge of domestic and international human rights laws, but is willing to comply with them.

(1)(b) Authorisation may be granted in relation to grounds expressly stated by the law. This means that there should be a clear connection between the grounds that may empower the application of such discretions and the decision taking of the Higher Authorising Authority.[86]

2.4.3 Article 7 The Designated Authorising Authority

The Designated Authorising Authority may be a public official or public authority acting on behalf of the executive. The authority should, in view of the categorisation proposed and the proportionality test to be applied, have at least a working knowledge of domestic and international human rights law.[87]

(1)(a) The Designated Authorising Authority may authorise Category II SPDG. It is the reasonableness test which should be applied in order to reveal whether SPDG is suitable, necessary and proportionate in the particular circumstances of the case.[88]

(1)(b) For an analogous explanation see subparagraph *(1)(b)* of Paragraph 2.4.2 above.[89]

2.4.4 Article 8 Formalities

(1) Authorisations for SPDG should generally be made in writing or electronically.[90]

(2) However, in exceptional urgent circumstances it may be necessary to authorise secret personal data gathering orally. The circumstances in which an oral authorisation may be appropriate could include those where there is an immediate threat to life such that a person's life might be endangered if the application procedure were undertaken in writing from the outset. After the period of urgency, the normal written process should be completed.[91] This means that the record of

---

85 See part IV, chap A., art 22; see also cl, SDA, s 14(1); NSA, art 39; ISA, s 11(2); CP-CS, para 2.4 to 2.10; FISA para 1805(b).

86 Eg see cl, SDA, s 14; NSA, art 34; ISA, s 11(2); RIPA, s 32(3)(a).

87 Eg see cl, CP-ADCD, para 3.11.

88 See part IV, chap A., art 22.

89 Eg see cl, SDA, s 14(1); RIPA, s 28(3) and CP-ADCD, para 2.3; FISA, para 1805(3).

90 Eg see cl, SDA, s 10; NSA, art 40; ISA, s 11(2); CP-ADCD, para 3.22; FISA, para 1802(a)(1).

91 Eg see cl, SDA, s 28 to 30; NSA, art 49; RICA, s 23(8); CP-ADCD, para 3.42 to 3.45; FISA, para 1805(f).

authorisation should either be created at the time of the oral authorisation or retrospectively at a date and time when reasonably practicable.

2.4.5 Article 9 Record Keeping of Authorisations

Two separate records are necessary. The first regards record keeping of applications,[92] and the second, record keeping of authorisations.[93] The fact that two records are kept separately enables constitutional oversight through cross-examinations. As stated in Part VII, Paragraph 2.2.2, record keeping is closely associated with the doctrine of checks and balances. In order to make a public authority accountable for the carrying out of its powers, or omissions to act, evidence is required.

(1)(a) to (c) For an analogous explanation see Part VII, Paragraph 2.2.2.

(1)(d) Again, for an analogous explanation see Part VII, Paragraph 2.2.2.

(1)(e) The authorising authority should also record why it agrees or disagrees that SPDG is reasonable in the particular circumstances of the case.[94] A later evaluation could, in view of this information recorded under Subparagraph *(1)(e)* and *(1)(d)* of this Paragraph, reveal whether the authorising authority had reasonable grounds to believe that SPDG was necessary, suitable and proportionate.

Indications as to sections *(1)(f) to (h)* should state whether a particular application was approved or disapproved. SPDG may, for whatever reason, be carried out despite its disapproval. Again, the making known of the authority by whom, and the date and time when SPDG was approved or disapproved provides important evidence.

(2) For an analogous explanation see Para 2.2.2 of Part VII.

2.4.6 Article 10 Renewal of Authorisations

An authorisation may require renewal in the light of the fact that an initial authorisation is limited by time, and a specific investigation or operation has not been completed at the moment the particular authorisation expires. Thus, renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future.

---

92 See generally part VII, para 2.2.2.

93 As covered under this para.

94 See part IV, chap A., para 22.

(1)(a) and *(b)* The renewed authorisation should be limited to a reasonable period of time. The authorising authority should specify the shortest period in which the objective for which the personal data is sought can be achieved.[95] To do otherwise will impact on the proportionality of the authorisation and impose an unnecessary burden upon the public authority conducting the covert investigation or operation.
(1)(c) The application for renewal should be made in writing or electronically. An oral application for a renewal is not necessary as the applying authority keeping records of any authorisation can choose the appropriate time for a renewal. In this respect there will be no urgent cases.

2.4.7 Article 11 Record Keeping of Renewable Authorisations

(1) For an analogous explanation see Part VII, Paragraph 2.2.2 and 2.4.5.

2.4.8 Article 12 Withdrawal of Authorisations

Where an authorisation becomes unnecessary, unsuitable, or is no longer proportionate to what is sought to be achieved, the authorisation should be withdrawn.
(1) The authority that authorises SPDG is also the authority that may revoke such authorisation. This recommendation requires a continued exchange of information regarding the advancement of a particular investigation or operation.[96]

2.4.9 Article 13 Record Keeping of Withdrawn Authorisations

(1) For an analogous explanation see Part VII, Paragraph 2.2.2 and 2.4.5.

3. Basic Proposal of International Application

3.1 Public Authority Sending Secretly Gathered Personal Data

3.1.1 Article 14 Privacy Compliance, Query of the Sender Public Authority

It should be stressed that the Basic Proposal of International Application covers the circumstance where a public authority receives a direct request for assistance from their counterparts in other countries,[97] or where a public authority considers by itself

---

95 Eg see cl, SDA, s 19; ISA, s 11(4); CP-ADCD, para 3.33.

96 Eg see cl, SDA, s 20, CP-ADCD, para 3.36.

97 The so-called non-judicial cooperation. This represents an exception to the general definition of a "public authority" as stated in part I, chap A., para (1)(e) and includes any person certain of whose functions are of a public nature only.

that a transferral of secretly gathered personal data is necessary, suitable, and proportionate to have it sent to a foreign recipient public authority. However, the recommendations do not cover the situation where a public authority receives a formal request from a foreign court or other prosecuting authority that appears to have a function of making requests for legal assistance.[98]

(1) Adequate protection may be assumed if the State in question incorporated the guidelines set forth in this paper as well as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980. Adequate protection to the right to privacy may also be given if a State ratified similar provisions which protect the right to privacy equally. Nevertheless, the public authority sending the secretly gathered personal data should decide in each case, and before transferring the data to the foreign recipient public authority, not only whether the data will be adequately protected there, but whether it is reasonable to transfer that data in the circumstances of the case.[99] For purposes of convenience, there should be a list drawn up of States that guarantee adequate privacy protection in respect of SPDG. This information may be deposited with an international organisation and should be made accessible to public authorities around the world.

3.1.2 Article 15 Exceptional Transfer Due to Substantial Public Interest

(1) Secretly gathered personal data should not be transferred unless the transfer is reasonable, the data is protected adequately, or there is a substantial public interest. Articles 15 and 14 must thus be read and given effect in correlation with each other. It will not always be possible to ensure adequate data protection by the public authority receiving the data. Exemptions to Article 14 of the guideline are necessary where the interest is public and substantial.[100] The interest is public if it concerns the people as a whole, and substantial if it is of considerable importance such as the protection of life. The consideration of the public authority sending the secretly gathered personal data is reasonable provided that the reasonableness test under Part IV, Chapter A., Article 22 of this guideline is satisfied.

3.1.3 Article 16 Record Keeping by the Sender Public Authority

---

98 The so-called judicial cooperation.

99 See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), part three, para 15.

100 Eg see CP-ADCD, para 6.19.

For explanation as to the general idea of record keeping see Part VII, Paragraph 2.2.2.

(1)(a) to (d) The record should contain a description of the secretly gathered personal data which were transferred, the name of the public authority sending and receiving the secretly gathered personal data, and the date and time the data was sent and received. The global quality of intelligence information can be improved by the fact that erroneous data gathering can be traced back. Without meticulous record keeping, errors cannot be corrected on a later date.

(1)(e) Article 16 of this guideline requires direct cooperation between public authorities that transfer secretly gathered personal data across borders. This would, for instance, mean that the public authority sending the data inquires into the purpose for which the data will be used. It would, in addition, require that the public authority sending the data could reasonably conclude that the transfer is necessary, suitable and proportionate in the light of the data content and the purpose for which it is sought and subsequently used. In terms of practical feasibility and rising administrative costs, such a test should not be overly stringent but merely block transborder flows of personal data that are obviously sent in contradiction of the general understanding of reasonableness.[101]

(1)(f) The record should indicate whether adequate protection is provided. This would mean that the record makes known whether the State to which the personal data is transferred has ratified data protection laws which comply with this guideline.

(1)(g) The public authority sending the secretly gathered personal data should state the reasons why it considers the transfer to be of substantial public interest in the particular circumstances of the case.

3.2 The Public Authority Receiving Secretly Gathered Personal Data

3.2.1 Article 17 Privacy Compliance, Query of the Recipient Public Authority

(1) An Article 17 privacy compliance query is *prima facie* expensive in view of a rise in administrative costs. However, as stated under Part VII, Paragraph 3.1.1, provided that the international privacy community produced a list with information about the privacy compliance of each country, the requirement set forth in Article 17 could be implemented without generating exorbitant costs. But certainly the time and energy

[101] See part VII, para 4.1.1.

needed to develop such a list will remain.[102] It should also be kept in mind that a complete disclosure of domestic laws by responsible Governments may encourage others to follow suit. The second sentence of Article 17 would require the public authority to apply the reasonableness test set forth under Article 22 of this guideline.

3.2.2 Article 18 Exceptional Receipt and Special Personal Data Marking

Article 18 provides, like Article 15, an exception to the general rule set forth in Article 17. A substantial public interest should in any case outweigh the right to privacy.

(1) Article 18 covers not only the situation where a recipient authority receives secretly gathered personal data from the sender public authority that actually acquired the data, but the circumstance where such data is passed across frontiers from one public authority to another.

(2) The idea behind the special marking of secretly gathered personal data is twofold. Firstly, the mark indicates that the data in question were acquired in a manner that may have infringed the privacy rights of the data subject. Public authorities should contemplate that whenever they receive secretly gathered personal data form foreign Governments they are likely to become the data controllers of that particular data. According to the *Accountability Principle*[103] of the OECD Privacy Guideline, a data controller should be held accountable for complying with measures which give effect to privacy laws such as Article 17 of CCPR. Secondly, the marking of personal data should provide a data quality indication. It can reasonably be assumed that a covert operation or investigation which is thoroughly tested against its necessity, suitability, and proportionality in one or more instances, and by one or more national public authorities, produces more concise and reliable intelligence information, than covert operations and investigations that gather personal data at will, that is to say, devoid of testing its actual reasonableness.[104]

---

[102] It should be suggested that the required research could be conducted by a non-governmental organisation such as Privacy International that has more than two decades of experience in this area of law. Privacy International <http://www.privacyinternational.org> accessed 13 May 2006

[103] See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), part two, para 14.

[104] When considering the UK Report of the Intelligence Service Commissioner for 2003, HC (2004-07) 884 and the UK Report of the Interception of Communications Commissioner for 2003, HC (2004-07) 883 it seems as if the likelihood that public officials act *intra vires* is greater where they are under strict scrutiny. The Interception of Communications Commissioner states in para 32: “It is very important from the point of view of the public that I stress that none of the breaches or errors were deliberate, that all were caused by human or procedural error or by technical problems and that in every case either no interception took place or, if there was interception, the product was destroyed immediately on discovery of the error”.

3.2.3 Article 19 Record Keeping by the Recipient Public Authority

For an explanation as to the general idea of record keeping see Part VII, Paragraph 2.2.2.

(1)(a) to (d) For an analogous explanation see Part VII, Paragraph 3.1.3.

(1)(e) The explanation required under this subparagraph can be very succinct. As with the secret acquisition of personal data through a covert investigation or operation, the recipient public authority prior to making a claim for that data should consider its necessity, suitability, and proportionality in the particular circumstances of the case.

(1)(f) and *(g)* For an analogous explanation see Part VII, Paragraph 3.1.3.

3.3 Internationally Accessible Database of Secretly Gathered Personal Data

3.3.1 Article 20 Personal Data Filling

The Article 20 recommendation has been formulated as a consequence of the fact that secretly gathered personal data flows have greatly increased, and may grow even further at the time of renewed political tension and in the light of the fact that religious and cultural frictions are being exploited for violent ends. It is likely that the need for internationally accessible data bases which are filled with secretly gathered personal data will rise accordingly.

(1) Data filed in internationally accessible databases should meet at least the minimum standards set forth in this guideline.

3.4 Transborder Liberalisation of Secretly Gathered Personal Data

3.4.1 Article 21 Transborder Liberalisation

(1) As stated in the Preface of this guideline the recommendations endeavour to strengthen the notion of free transborder information flows. The guideline has *inter alia* as its objective the elimination of the reasons which might prompt governments to restrict transborder flows of secretly gathered personal data.[105] Article 21 calls on Governments to waive additional privacy laws which could impede the effective prevention of terrorism and serious crime.

[105] See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980), part three, para 17 and 18.

4. Basic Proposal of International and National Application

4.1 Reasonableness

4.1.1 Article 22 The Test

Any action which *prima facie* violates protected rights should be justified on the basis that the infringement is justifiable on the grounds set forth by law. Thus, generally speaking, the action taken or to be taken must be judged according to whether or not that action was proportionate to the objective behind the action. [106]

(1)(a) to (b) The reasonableness test in the light of SPDG involves balancing the extent of the intrusiveness of the interference with an individual's right to privacy against a specific benefit to the investigation or operation being undertaken by the relevant public authority, and in the public interest.[107] This includes consideration of any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation. An interference with privacy and individual liberties may still not be justified because the collateral damage caused by a covert operation or investigation is regarded as overly severe.[108]

The test whether an authority's act or omission is reasonable or not should be an objective one. The standard against which the authority's conduct or omission to act should be measured is that of a fictitious reasonable authority. Thus, the test cannot be satisfied unless a fictitious and reasonable authority would have acted equally under the same circumstances of the case.

(2) Accountability plays a pivotal role in the enforcement of the recommendations introduced under this guideline. Arbitrary and unlawful SPDG should be sanctioned by the States according to their severity, and in view of the particular circumstances of the case.[109]

5. National Implementation

The detailed implementation of the guideline would be left, in the first place, to the States. This is bound to vary according to different legal systems and traditions. The

---

[106] This recommendation should apply to any executive act or omission covered under this guideline.

[107] See UNHRC "General Comment 16" (8 April 1988), para 4.

[108] Eg see cl, CP-CS, para 2.6 to 2.10.

[109] Eg see cl, ISA, s 39(a).

guideline attempts merely to establish a general framework indicating in broad terms what kind of national machinery is envisaged for putting the Guideline into effect.
An alternative solution to the multinational incorporation of this guideline would be that the States that exchanged secretly gathered personal data contracted bilaterally on the recommendations set forth in this guideline.
(1)(a) Countries are invited to adopt appropriate domestic legislation. The word “appropriate” foreshadows that it is the judgment of individual countries as to what can be regarded as appropriate or not.
(1)(b) This paragraph is dealing with discrimination and is directed against unfair practices such as unfair discrimination on the basis of nationality and domicile, race, and sex in the fight against terrorism and serious crime.

6. International Cooperation

The provision on national procedures assumes that the guideline should form a basis for continued cooperation.
(1) As indicated in Part VII, Paragraph 2.3, the categorisation in this guideline is a recommendation only and it will be for the States acting together to find a suitable segmentation for SPDG.
(2) Procedures should not hamper the free flow of secretly gathered personal data as they have to be responsive to the level of threat posed.
(3)(a) Procedures to facilitate personal data exchange should, if possible, become common practice on an international level.
(3)(b) Mutual aid in investigatory matters should be stepped up. Its practical significance is likely to grow in view of global instability.

Part VIII - Conclusion

1. Considerations in the Narrow Sense

According to the English philosopher Thomas Hobbes (1588-1679), the motive and end for which people renounced and transferred their natural rights to an authority is nothing else but security of person.[110] In thinking of the people as *homo homini lupus*,[111] it is the State's prime duty to preserve security, stability and justness among its citizens. Terrorism that has as its objective the spread of fear and mayhem deprives the people of the very benefit they have theoretically contracted for, namely the surrendering of just enough of their natural rights for the authority to be able to ensure internal peace and a common defence.[112]

In order to guarantee that the thesis of the Hobbesian social contract is upheld among democracies around the world, the UN Security Council called upon States[113] to provide its public authorities with wide discretion to tackle terrorists and other perpetrators before they strike or commit a crime. Such powers are *inter alia* the carrying out of covert surveillance in residential premises or private vehicles, listening to calls made on a particular telephone, or opening and reading the content of a person's letter or e-mail message. They include also the use of agents who are members of, or act on behalf of the Government to obtain personal information from people who do not know that this information will reach public authorities. Some countries allow public officials to demand and obtain information and documents from aircraft and ship operators. Nowadays it is also common Government practice for records of book lending or information as to the use of credit cards to be compiled covertly.[114]

Naturally, such powers may also cause adverse effects. A single person or group of individuals can become enticed to systematically record and observe the movements

---

[110] See T Hobbes, *The Leviathan* (Andrew Crook, at the Green Dragon in St. Paul's Church-yard, London 1651), part I, chap XIV.

[111] *Homo homini lupus*, Latin for "the wolf in every person". Hobbes saw the life of men from an anthropological point of view as being as poor, nasty, and brutish as that of a beast. In this state of nature, each person has a right to everything in the world (*ius in omnia*), thereby producing a constant and right-based war of all against all (*bellum omnium contra omnes*). However, in renouncing and transferring the natural rights of men to the authority, security and peace can and should be guaranteed by a single authority. Ibid.

[112] Ibid.

[113] See generally UNSC Res relevant to terrorism and serious crime at UNSC, "Counter-Terrorism Committee" < http://www.un.org/sc/ctc/resolutions.shtml > accessed 13 May 2006

[114] For a general overview see part X, para 1.

and contacts of others. Undoubtedly, personal data in today's interrelated and interdependent information-hungry world is exceedingly useful if applied strategically. And where there is such a concentration of powers, it can be misused, unless there is an effective and equilibrated mechanism of control[115] and oversight.[116]

Thus, central to this guideline is the categorisation of personal data. At this stage the actual segmentation into (i) intrusive and intimate SPDG, (ii) non-intrusive and non-intimate SPDG, and (iii) open source SPDG should not be read rigidly.[117] The idea in stating several sources of international human rights interpretation is that the categorisation proposed should provide a basis for discussion. What other way would there be to find an internationally applicable privacy framework that can accommodate different approaches to privacy, tailored to national legal and cultural norms, and that will enable global information flows while respecting those norms? It is possible that States are *a fortiori* willing to find a suitable categorisation for a minimum standard of SPDG if it were in line with recommendations set forth by a universally accepted institution. In having regard to the newly established UN Human Rights Council,[118] such proposals may be discussed soon.

The second pivotal concept is the legal authorisation procedure which enables covert investigations and operations in specific circumstances of a case. In this paper particular heed has been paid to the freedom of action in view of country-specific incorporations. Domestic and cultural traditions and values must be respected when considering the meaning and scope of human rights.[119] The distribution of powers as well as the system of checks and balances compared between States may differ. Where in one country may be considered more appropriate to have a Minister[120] to authorise SPDG, it may be a judge or special tribunal[121] holding such discretion in another. The approach applied in this guideline represents a minimum standard for the protection of privacy and individual liberties. States that desire to guarantee

---

115 See generally part II to IV.

116 See part X, para 2.

117 See part VII, para 2.3.1.

118 See UNGA Res 60/251 (3 April 2006) UN Doc A/RES/60/251.

119 See part VII, para 2.4.1 and 2.4.2.

120 Common law countries, for instance, have a longstanding tradition of individual responsibility for personal conduct of public officials. The public is entitled to expect very high standards of behaviour from ministers, as they have profound influence over the daily life of the citizens. If they do not meet such standards they must resign. See Nolan Report, "Standards in Public Life" (Cm 2850-I, 1995, London: HMSO), chap 3, para 4.

121 See eg n 6 above; see also U Häfelin / W Haller, *Schweizerisches Bundesstaatsrecht*, (5. Auflage, Schulthess Juristische Medien AG, Zürich 2001), para 1650.

further protection, for instance in having any application for SGPD vetted by an independent judge or tribunal, are encouraged to do so, but they should not restrict countries that agree only to the minimum standard proposed under this guideline. In each State the level of threat varies greatly and so does the quantity of covert operations and investigations conducted. Arguably, it would make little sense in respect of the effectiveness of crime and terrorism prevention if SPDG had compulsorily to be authorised by a judiciary that could never absorb the amount of applications brought. Once the proposed system of control is incorporated into domestic laws, it shall not hinder the working of the administration.

The third concept is not of lesser importance. It concerns recommendations with the objective of intensifying and accelerating the exchange of secretly gathered personal data for protection from terrorism and serious crime.[122] At first glance, the legal information sharing requirement in compliance with SPDG standards[123] seems more of a block than an aid to information exchange. Such a conclusion cannot be contested if the Basic Proposals of International Application of Part III were understood as being incorporative in today's international privacy environment. So, for instance, where a foreign recipient public authority cannot guarantee adequate privacy protection, and the data transfer is not of a substantial public interest, that data should not be transferred.[124] It must therefore be emphasised that the proposals in this guideline have been made prospectively. Nevertheless, they could be implemented via bilateral agreements until an international standard for privacy protection in respect to SPDG is found. Once the Basic Proposals of National Application of Part II are built into domestic legal systems, transborder flows of secretly gathered personal data could be free in their entirety.

It will still be necessary to keep records because where erroneous personal data gathering may provoke a chain of negative effects, a trace of the records[125] and subsequent data correction can protect the privacy and other fundamental human rights of innocent individuals.[126] The carrying out of such laborious and time-consuming data tracing is unreasonable where the matter concerned is trivial, or

---

[122] See part III, chap D., art 21.

[123] See part III, chap A., art 14 and 15, chap B., art 17 and 18.

[124] See part III, chap A., art 14 in correlation to art 15.

[125] See part III, chap A., art 16, chap B, art 19.

[126] Such as arrests and detentions of innocent individuals caused by erroneous intelligence information.

where there is an imbalance between the work to be conducted and the results to be achieved.

To sum up, although the proposed mechanisms of control,[127] record keeping[128] and legal compliance queries[129] undoubtedly raise costs in one way, they are likely to reduce them in another. Administrative control via an authorisation system reduces the number of expensive covert operations and investigations undertaken by public officials if reasonably tested against their necessity, suitability, and proportionality in the particular circumstances of a case. In this respect it can be stated that all three concepts together[130] increase the quality of intelligence information. They thereby enable Governments to inquire into, and take measures against genuine threats of terrorism and serious crime. Heed should particularly be paid to the fact that counter-terrorism measures can be very costly if people are harmed and property is damaged mistakenly.

2. Considerations in the Wider Sense

In contemplating the costs which are generated by covert operations and investigations, the necessity of systems of control and oversight, and the accompanying risks of human rights infringements, it is desirable to look beyond what is considered to be the sphere and discipline of law.[131]

Three prime examples of transdisciplinary questions are: *(a)* Will the proposed mechanisms of authorisation stop public officials interfering with the right to privacy arbitrarily or unlawfully? (That is to say, are the recommendations formulated and enforced in a manner that the public officials addressed are able and willing to comprehend the norms, and act according to them?) *(b)* Will the secret acquisition of personal data and subsequent exchange across borders bring the desired results? (Can terrorism and serious crime be prevented by covert operations and investigations which may lead to an arrest of a dangerous person before he or she has the time to activate a bomb or commit another serious crime?) *(c)* Or, should more attention be paid to the deep rooted disagreements between human beings

---

127 See part II, chap D., art 5 and 6.

128 See part II, chap B., art 3, chap D., art 9, art 11, art 13, and part III, chap A., art 16, chap B., art 19.

129 See part III, chap A., art 14 and 15, chap B., art 17 and 18.

130 See n 127 to 129.

131 See generally P Richli, *Interdisziplinäre Daumenregeln für eine faire Rechtsetzung* (Helbing & Lichtenhahn Verlag, Basel 2000), p 13 ff.

which can only be tackled by activities that are individually tailored to solve the actual causes of conflict rather than merely strengthening what is considered to be the fight against their repercussions?[132]

The complexity of these questions is devoid of limits by which they could be considered in rudimentary terms only. The idea of this part is to encourage professionals in disciplines other than law to discuss the issues raised and work towards realizable solutions which have as their objective the guarantee and development of secure, just, and tolerant societies. This paper addresses question *(a)* and *(b)* briefly, but will look at question *(c)* in more detail.

(a) Will the proposed mechanisms of authorisation stop public officials interfering with the right to privacy arbitrarily or unlawfully? As a general rule it can be stated that an effective incorporation would *inter alia* not only require that legal provisions are worded clearly, precisely, and coherently,[133] but that principles are enforced effectively.[134] Public officials must be able and willing to construct the actual meaning of a particular provision. Their willingness may depend on two factors. Firstly, they must be fully aware of the system of sanctions that will come rigorously into effect if they act *ultra vires*. Secondly, and in many instances more importantly, the protection of human rights depends on individual and collective ethics of care and of legal adherence. Public officials should be taught the meaning and scope of human rights. They will be required to see and comprehend the necessity of such fundamental values. And ideally, they will begin to consider themselves as the keepers of justice and right. What should never be forgotten is that "*a legal provision has no greater force than that which the persons in authority are willing to attribute to it*."[135]

(b) Will the secret acquisition of personal data and subsequent exchange across borders bring the desired results? Last year saw 11,000 terror attacks worldwide and 14,600 deaths[136] despite the incorporation of 13 international legal instruments[137]

---

[132] One could see in counter-terrorism measures a mere fight against the repercussions of human conflict.

[133] See G Müller, *Elemente einer Rechtssetzungslehre* (Schulthess Juristische Medien AG, Zürich 1999), p 146 ff.

[134] A public authority or individual public official that acts contrary to the Reasonableness Test should be held accountable. See part IV, chap A., art 22.

[135] A famous English legal proverb by an unknown author.

[136] See United States Department of State Publication, Office of the Coordinator for Counter-Terrorism "Country Report on Terrorism" (April 2006), p 287.

[137] See generally Internationally Applicable Counter-Terrorism Convention and Protocols at UNSC, "Counter-Terrorism Committee" <http://www.un.org/sc/ctc/law.shtml> accessed 13 May 2006

that should prevent terrorism and serious crime. But in studying domestic criminal statistics such as the US Source Book of Criminal Justice[138] or the UK's Development Research Statistics,[139] it can be deduced that in both countries there has been a significant decrease in murder and non-negligent manslaughter, rape, robbery, and aggravated assault cases in recent years. In Australia the number of offences against the person has decreased slightly from 118,903 in 2003 to 117,500 offences in 2004,[140] and according to the South African Police Service, crime levels there have stabilised[141] over the past few years. Not so in Switzerland, where statistics[142] show that the number of criminal offences has increased by approximately 25 percent since the year 2000.[143]

With regard to these figures no clear picture emerges. The effectiveness or ineffectiveness of measures in the fight against terrorism and serious crime is unclear. Moreover, governments release statistics about the number of foiled terror attacks and arrests made in connection with terrorism and serious crime very sparingly.

Turning our attention to the transdisciplinary question at *(c),* and in view of the statistics highlighted above, it cannot be wrong to reflect on the possible grounds for terrorism and serious crime before considering the actual measures to tackle them. Thomas Hobbes embarks on the theory that either because of personal beliefs or because of external influences, disagreement among individuals must be regarded as a natural consequence of their existence. [144]

What makes, however, a disagreement become serious and escalate? The majority of today's conflicts arise between different ethnic, religious, and economic groups.

---

138 The average rate of serious crime fell by approx 17% from 1998 to 2004. See US Bureau of Justice Statistics, "Sourcebook of Criminal Justice Statistics 2004" <http://www.albany.edu/sourcebook/pdf/t31062004.pdf> accessed 19 May 2006

139 The average rate of violent crimes fell by approx 35% from a peak in 1995 to 2005. See UK Home Office, "Research Development Statistics 2005" < http://www.homeoffice.gov.uk/rds/pdfs05/hosb1105.pdf> accessed 19 May 2006

140 See Office of Crime Statistics and Research of Australia as to the year 2004 <http://www.ocsar.sa.gov.au> accessed 19 May 2006

141 See South African Cape Gateway, "Statistics as to the year 2004 to 2005" <http://www.capegateway.gov.za/eng/pubs/public_info/C/86878/1> accessed 19 May 2006

142 See Office Féderal de la Statistique as to the year 2000 to 2005 , "Infraction Lois" <http://www.bfs.admin.ch> accessed 19 May 2006

143 It must, however, be noted that Swiss law enforcement officers have at present, unlike public officials of the other countries vetted in the comparative legal research part, no means to intercept communications and conduct intrusive surveillance. See part X, para 1.

144 See n 110 above; see also C Darwin, *The Expression of the Emotions in Man and Animals* (John Murray, London 1872).

They escalate not only because of unsatisfied material desires,[145] the unequal separation of powers, and an inequitable access to resources, but also because of an insufficiency in, or a complete lack of, security, identity, acceptance, autonomy and dignity.[146] Culture can play a pivotal role when it comes to serious disagreements. Not long ago, culture was interpreted to mean the special achievements of a nation in art, music and architecture. Nowadays culture can be defined as a system of mutual belief, religion, common practices and norms which vary from one nation or region to another.[147] American anthropologist Melville Jean Herskovits (1895-1963) described culture as "the man-made part of the human environment".[148]

The capability of self-reflection and the consciousness of one's own mortality[149] can be seen as a continuous source of existential anguish.[150] According to the Terror Management Theory,[151] culture in the modern sense diminishes this psychological terror by providing meaning, organisation and continuity to men and women. Compliance with particular cultural values and norms enhances the feeling of security and self-esteem, provided that the individual is capable of living in accordance with the cultural standards of his or her community. Belief in the rightness of these cultural values and standards creates the conviction to live a reasonable and meaningful life. Because of this, men and women strive to have their cultural worldview confirmed by others, thereby receiving the community's estimation and respect.

However, whenever one's worldview is threatened by the *Weltanschauung*[152] of another individual, it means that one's self-respect is endangered as well. In such circumstances people not only endeavour to deny or devaluate the importance of the other worldview, but try to controvert those ideas and opinions.[153] Differing

---

145 Caused by an unjust distribution of goods.

146 See H Kelman, Interactive Problem Solving as a Metaphor for International Conflict Resolutions: Lessons for the Policy Process, *Peace and Conflict* (Journal of Peace Psychology, 1999), p 201-218.

147 See G Bierbrauer, *Interkulturelles Verhandeln* (F. Haft v. Schlieffen (Hg.), Handbuch Mediation, München 2002), p 266-288.

148 See M J Herskovits, *Man and His Works: The Science of Cultural Anthropology*, (New York 1948).

149 This is believed to be uniquely reserved to humans.

150 See E Becker, Dynamik des Todes, *Die Überwindung der Todesfurcht – Ursprung der Kultur* (Freiburg 1976).

151 See S Solomon / J Greenberg / T Pyszczynski, *A Terror Management Theory of Social Behaviour* (The Psychological Functions of Self-Esteem and Cultural Wold Views, Mark P. Zanna (ed.), Advances in Experimental Social Psychology, 1991), p 93-159.

152 Weltanschauung, German for "a particular philosophy or view of life".

153 See n 151 above.

worldviews between two persons or a group of individuals may for these reasons produce anger and hatred, and in the worst scenario create the desire for the complete destruction of others' existence.[154]

The question of paramount importance which arises after following the above line of reasoning is: how can the escalation of attacks on people's perceptions and convictions be kept within the bounds of a State's internal and external security, stability, and peace? According to the German philosopher Georg Wilhelm Friedrich Hegel (1770-1831) the State is required to regulate between individuals. To him it is *Anerkennung*[155] through reasoning which creates the willingness of individuals to tolerate a difficult or unpleasant situation. However, Immanuel Kant (1724-1804) was of the opinion that it is not primarily the State's duty to encourage and control the willingness to tolerate, but to leave it up to the people to reason and determine for themselves. To him, individuals understand through their autonomous reasoning "*to act only according to that maxim by which they can at the same time will that it would become a universal law*."[156]

If we combined the two philosophies in a synthesis, it could in general terms be said that the State should not interfere, but allow reason to prevail as long as people understand that their actions are to be taken in ways that would be equitable to them if taken by others.[157] However, at a time of renewed religious and cultural frictions, and in instances where conflicts are exploited for violent ends, it must be concluded that people are to a certain extent unable to regulate themselves. It is thus the State's obligation to intervene in this sphere of powerlessness and re-establish security, stability, and justness among the people.

Are State institutions able to overcome such difficulties on their own? In other words, can they encourage citizens to find their inner willingness to accept varying cultural and religious traditions and truths?

In thinking about our interrelated, interdependent, and intercultural world, it seems unlikely that dialogue and its accompanying actions on a purely secular basis will be

---

[154] See generally G Bierbrauer, *Triebe, Instinkte, Kultur und Todesangst* (Osnabrücker Jahrbuch Frieden und Wissenschaft, Göttingen, Universität Osnabrück 2003), p 137-146.

[155] Anerkennung, German for „acceptance", see generally G W F Hegel, *Grundlinien der Philosophie des Rechts* von 1820 (Helmut Reichelt, Ullstein-Buch, Frankfurt am Main 1972).

[156] See generally I Kant, Essay Beantwortung der Frage: *Was ist Aufklärung* (Berlinische Monatsschrift, Johann Erich Biester und Friedrich Gedike, Berlin 1784).

[157] A reformulation of the golden rule or ethic of reciprocity. For a list of uses see Wikipedia, the Free Encyclopaedia, "Ethic of Reciprocity" <http://en.wikipedia.org/wiki/Main_Page> accessed 13 May 2006

sufficient. In order to overcome the difficulties of the 21st Century, intercultural and inter-religious exchange is required. The interest in discovering human richness in thought and appreciation should not, therefore, be limited to a mundane level, but be taken onto a spiritual one. Personally speaking, it is time not only to promote Hegel's *Anerkennung* and Kant's Categorical Imperative*,* but to simultaneously leap forward in creating a common desire for intercultural as well as inter-religious candour, *veracitas*,[158] respectfulness, and even admiration. It will be difficult – but it is the challenge we should finally face.

[158] Veracitas, Latin for "speaking truly".

Part IX - Summary

How should individuals who live their lives with complete integrity, enjoy family harmony and pursue an honourable occupation be unmasked as potential, internationally operating terrorists and perpetrators of other serious crimes if not by secretly listening to their telephone calls, opening and reading the content of their letters or e-mail messages, and exchanging that data across frontiers and between Governments?[159]

As pointed out in Part VII, Paragraph 1.4 to 1.6, this dilemma becomes apparent when considering the State's duty to prevent terrorism and serious crime on the one hand, and have respect for privacy and individual liberties on the other. The solution put forward in this paper is a compromise between these competing values. Part II, Basic Proposals of National Application, proposes a system of checks and balances that should not only enable governments to conduct SPDG, but prevent them from acting *ultra vires*.

In order that a government action can be regarded as checked and balanced, it must pass through the so-called *Montesquieuian* gauntlet.[160] Part II, Chapter D., Articles 5 to 7 provide the ability, right, and responsibility to a power, other than the one involved in the systematic and secret acquisition of personal data, to monitor the activities of the public authority actually carrying out covert operations and investigations. Although the guideline encourages the ability of each branch to use its authority to limit the powers of another branch, it recognises that it is the political and legal task of the individual State to decide how to keep each independent entity within its prescribed powers.[161]

Part III of the guideline has as its objective the elimination of the reasons which might prompt governments to restrict transborder flows of secretly gathered personal data. And in Part VIII the paper questions whether, in today's reality, traditional counter-terrorism measures are justifiable. Ultimately, it endeavours to provide an impetus for activities which focus directly on the causes of human conflict, thereby paving the way for secure, just and tolerant societies.

---

[159] For an anologous appeal see A Kölz / I Häner, *Nachdenken über den demokratischen Staat und seine Geschichte*, Aufsatz von Helen Keller, *Antiterrormassnahmen: Verfahrensschutz bei der Sperrung von Banknoten* (Schulthess, Zürich 2003), p 299 ff.

[160] See generally J. V. Prichard (tr), *De L'Esprit des Lois* (1748) de Charles de Secondat, Baron de Montesquieu (G. Bell & Sons, Ltd., London 1914).

[161] See part VII, para 2.4.1 to 2.4.3.

Part X - Appendices

1. Table of Prime Methods of Secret Information Gathering

COMPARATIVE LEGAL RESEARCH[162]	1. NON-INTRUSIVE SURVEIL-LANCE	2. USE OF AGENTS	3. ON DEMAND DOCUMENTS REQUESTS	4. INTERCEPTION OF COMMUNI-CATIONS	5. INTRUSIVE SURVEILLANCE
AUSTRALIA	X	X	X	X	X
MEXICO	X	X	X	X	X
SOUTH AFRICA	X			X	X
SWITZERLAND	X				
UK	X	X		X	X
USA	X	X	X	X	X

1. Non-Intrusive Surveillance – is covert surveillance but not intrusive surveillance under taken for the purposes of a specific investigation or operation in a manner likely to reveal private information about someone.

2. Use of Agents or Covert Human Intelligence Sources – are essentially people who are members of or act on behalf of one of the intelligence services to obtain information from people who do not know that this information will reach the public authorities.

3. On Demand Document and Information Request – allows investigators to demand and obtain information and documents from private entities. It includes for instance information and documents from an operator of an aircraft or ship, documents about the books a suspect has borrowed from a library, or credit-card records, which are relevant to a matter regarding terrorist or other criminal activities.

4. Interception of Communications – regards *inter alia* listening to calls made on a particular telephone or opening and reading the content of a person's letter or e-mails.

5. Intrusive Surveillance – is covert surveillance undertaken in residential premises or a private vehicle of the purposes of a specific investigation or operation in a manner likely to reveal private information about someone.

[162] Eg see cl, SDA, s 18; NSA, art 34; RICA, s 7(1)(c); FPNS, art 14(2); RIPA, s 28, 29, and 32; FISA, para 1801(f).

2. Table of Mechanisms of Control

COMPARATIVE LEGAL RESEARCH[163]	1. INTERNAL AUTHORISATION	2. EXTERNAL AUTHORISATION	3. NO AUTHORISATION
AUSTRALIA	X	X	
MEXICO		X	
SOUTH AFRICA	X	X	
SWITZERLAND			X
UK	X	X	
USA	X	X	

Mechanisms of control prevent unlawful and arbitrary SPDG before it can be carried out by public authorities. They can be separated into an “Internal Authorisation” and “External Authorisation” systems but should not be confused with mechanisms of oversight which are conducted after SPDG was carried out by public authorities.

1. Internal Authorisation – refers to an authorisation system which is conducted by the same branch of powers that is actually carrying out SPDG. An example of this is a Director of the Security Services who authorises SPDG.[164]

2. External Authorisation – refers to an authorisation system which is conducted by a branch of powers other than the public authority actually carrying out SPDG. An example of this is a judge who authorises SPDG.[165]

3. No Authorisation – refers to the fact that there is no mechanism of control in place. In having regard to the comparative legal research undertaken for this paper, this regards Switzerland only.[166]

[163] Eg see cl, SDA, s 14(1); NSA, art 39; ISA, s 11(2); CP-CS, para 2.4 to 2.10; FISA para 1805(b).
[164] Eg see cl, SDA, s 11.
[165] Eg see cl, NSA, art 34; ISA, s 11(2).
[166] See cl, FPNS, art 14(2)(a)-(g).

3. Table of Official Legislation Sources

	OFFICIAL INTERNET RESOURCES
AUSTRALIA	ATTORNEYS GENERAL'S OFFICE: HTTP://WWW.NATIONALSECURITY.GOV.AU
MEXICO	UNAM DATABASE: HTTP://INFO4.JURIDICAS.UNAM.MX/IJURE/FED
SOUTH AFRICA	LEGISLATION DATABASE: HTTP://WWW.INFO.GOV.ZA/ABOUTGOVT/DEPT.HTM
SWITZERLAND	LEGISLATION DATABASE: HTTP://WWW.ADMIN.CH/CH/D/SR/SR.HTML
UK	HOME OFFICE: HTTP://SECURITY.HOMEOFFICE.GOV.UK/NEWS-AND-PUBLICATIONS1
USA	LAW REVISIONS COUNCIL: HTTP://USCODE.HOUSE.GOV/SEARCH/CRITERIA.SHTML

4. Statement of Independence as to the Composition of this Paper

I hereby declare that this paper was composed without the help of third parties, and no sources other than the ones indicated were used. I am fully aware of the fact that in the event of plagiarism this paper would not be “recognised.”

Place …Lucerne – Switzerland.. Date……30 June 2006……

Signature……