UNITED
NATIONS

A

General Assembly

Distr.
GENERAL

A/HRC/13/37
18 December 2009

Original: ENGLISH

HUMAN RIGHTS COUNCIL
Thirteenth session
Agenda item 3

PROMOTION AND PROTECTION OF ALL HUMAN RIGHTS, CIVIL, POLITICAL, ECONOMIC, SOCIAL AND CULTURAL RIGHTS, INCLUDING THE RIGHT TO DEVELOPMENT

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin

Summary

The Special Rapporteur, in chapter I of the present report, lists his key activities from 1 August to 15 December 2009. The main report, contained in chapter II, highlights several concerns of the Special Rapporteur regarding the protection of the right to privacy in the fight against terrorism. The importance of the right to privacy and data protection is highlighted in section A.

Article 17 of the International Covenant on Civil and Political Rights is flexible enough to enable necessary, legitimate and proportionate restrictions to the right to privacy. The Special Rapporteur argues, in section B, that article 17 should be interpreted as containing elements of a permissible limitations test. In this context, he calls upon calls upon States to justify why a particular aim is legitimate justification for restrictions upon article 17, and upon the Human Rights Committee to adopt a new general comment on article 17.

The Special Rapporteur highlights the erosion of the right to privacy in the fight against terrorism in section C. This erosion takes place through the use of surveillance powers and new technologies, which are used without adequate legal safeguards. States have endangered the protection of the right to privacy by not extending pre-existing safeguards in their cooperation with third countries and private actors. These measures have not only led to violations of the right to privacy, but also have an impact on due process rights and the freedom of movement – especially at borders – and can have a chilling effect on the freedom of association and the freedom of expression.

Without a rigorous set of legal safeguards and a means to measure the necessity, proportionality and reasonableness of the interference, States have no guidance on minimizing the risks to privacy generated by their new policies. The Special Rapporteur has identified, in section D, some of the legal safeguards that have emerged through policymaking, jurisprudence, policy reviews, and good practice from around the world.

The concluding section makes recommendations to various key actors (domestic legislative assemblies, domestic executive powers and the United Nations) in order to improve the protection of the right to privacy in the fight against terrorism.

CONTENTS

		Paragraphs	*Page*
I.	INTRODUCTION	1-2	
II.	ACTIVITIES OF THE SPECIAL RAPPORTEUR	3-10	
III.	THE RIGHT TO PRIVACY	11-58	
	A. The right to privacy as enshrined in constitutions and international human rights treaties	11-13	
	B. Permissible limitations under the right to privacy	14-19	
	C. Erosion of the right to privacy by counter-terrorism policies	20-47	
	D. Best practices	48-57	
IV.	CONCLUSION AND RECOMMENDATIONS	58-74	
	A. Conclusions	58-59	
	B. Recommendations	60-74	

I. INTRODUCTION

1. This report is submitted to the Human Rights Council by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, pursuant to General Assembly resolution 63/185 and Human Rights Council resolution 10/15. The main report lists the activities of the Special Rapporteur from 1 August to 15 December 2009 and focuses thematically on the right to privacy as a human right in the counter-terrorism context. The addenda contain a communications report (A/HRC/13/37/Add.1) and a report on the fact-finding mission to Egypt from 17 to 21 April 2009 (A/HRC/13/37/Add.2).

2. Regarding upcoming country visits, the Special Rapporteur hopes to conduct a mission to Tunisia prior to presenting this report. The Special Rapporteur has suggested dates in late January and early February 2010 and is awaiting a response from the Government. The Special Rapporteur also hopes to conduct official visits to Chile and Peru in 2010. There are outstanding visit requests for Algeria, Malaysia, Pakistan, the Philippines and Thailand.

II. ACTIVITIES OF THE SPECIAL RAPPORTEUR

3. On 18 and 19 September 2009, the Special Rapporteur convened an expert group meeting at the European University Institute in Florence to discuss thematic issues related to his mandate.[1] The meeting partly coincided with a public event on the "Fight against Terrorism: Challenges for the Judiciary", jointly organized with the Venice Commission and the Sub-Committee on Crime Problems of the Council of Europe. The event was co-funded by the Åbo Akademi University Institute for Human Rights, through its project to support the mandate of the Special Rapporteur.

4. On 29 and 30 September 2009, the Special Rapporteur, along with the other mandate holders involved, participated in informal consultations in Geneva regarding a global joint

[1] The Special Rapporteur is grateful for the assistance of the members of the expert panel, Dr. Gus Hosein and his research assistant Mathias Vermeulen and the participants of his PhD candidate seminar at the European University Institute, in producing this report.

study on secret detention (A/HRC/13/42). He also met with representatives of the Permanent Missions of Egypt and Tunisia in regard to country visits conducted or planned.

5. On 2 and 3 October 2009, the Special Rapporteur participated in a Wilton Park Conference on "Terrorism, security and human rights: opportunities for policy change" and was a panelist for the discussion on the role of international organizations in response to terrorism and the protection of human rights.

6. On 4 October 2009, the Special Rapporteur delivered a keynote address on the occasion of the inauguration of the academic year at the Faculty of Law at the University of the Basque Country (Universidad del País Vasco) in Bilbao, Spain.

7. From 12 to 14 October 2009, the Special Rapporteur participated in two events in Vienna: the International Workshop of National Counter-Terrorism Focal Points and the Counter-Terrorism Implementation Task Force (CTITF) Retreat. The workshop was jointly organized by a number of Member States and United Nations Office on Drugs and Crime, in close cooperation with the CTITF Office and the Counter-Terrorism Executive Directorate (CTED). It provided a forum to exchange views on how to better link global and national counter-terrorism efforts by fostering greater networking among national counter-terrorism focal points and facilitating their role as interface between national, regional and global counter-terrorism efforts. The CTITF retreat focused on ways forward to expand and strengthen partnerships between Member States, the United Nations system, regional and other organizations and civil society in implementing the United Nations Global Counter-Terrorism Strategy.[2]

8. On 20 October 2009, the Special Rapporteur was represented at a seminar in Brussels on "Strengthening the UN Targeted Sanctions through Fair and Clear Procedures", organized by the Belgian Federal Public Service for Foreign Affairs, Foreign Trade and Development Cooperation.

[2] See General Assembly resolution 60/288.

9. From 26 to 28 October 2009, the Special Rapporteur was in New York to present to the Third Committee of the General Assembly his report,[3] which focused on the gender impact of counter-terrorism measures. The Special Rapporteur had a formal meeting with the Al-Qaida and Taliban Sanctions Committee of the Security Council and met with the Director of the Counter-Terrorism Executive Directorate (CTED). The Special Rapporteur was a panelist at a side event "Engendering Counter-terrorism and National Security" hosted by the Centre for Human Rights and Global Justice of the New York University School of Law. He also met with a number of non-governmental organizations and gave a press conference.

10. On 29 October 2009, the Special Rapporteur met with the Assistant Secretary for Democracy, Human Rights and Labor and other officials of the United States State Department in Washington, D.C., to discuss current and future legal developments with the new Administration, in follow-up to his visit to the United States of America in 2007,[4] and more general issues concerning international humanitarian and human rights law in the counter-terrorism context.

II. THE RIGHT TO PRIVACY

A. The right to privacy as enshrined in constitutions and international human rights treaties

11. Privacy is a fundamental human right that has been defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others and free from State intervention and free from excessive unsolicited intervention by other uninvited individuals.[5] The right to privacy has evolved along two different paths. Universal human rights instruments have focused on the negative dimension of the right to privacy, prohibiting any arbitrary interference with a

[3] A/64/211.

[4] See A/HRC/6/17Add.3.

[5] Lord Lester and D. Pannick (eds.), *Human Rights Law and Practice* (London, Butterworth, 2004), para. 4.82.

person's privacy, family, home or correspondence,[6] while some regional and domestic instruments have also included a positive dimension: everyone has the right to respect for his/her private and family life, his/her home and correspondence,[7] or the right to have his/her dignity, personal integrity or good reputation recognized and respected.[8] While privacy is not always directly mentioned as a separate right in constitutions, nearly all States recognize its value as a matter of constitutional significance. In some countries, the right to privacy emerges by extension of the common law of breach of confidence, the right to liberty, freedom of expression or due process. In other countries, the right to privacy emerges as a religious value. The right to privacy is therefore not only a fundamental human right, but also a human right that supports other human rights and forms the basis of any democratic society.

12. The State's ability to develop record-keeping facilities was enhanced with the development of information technology. Enhanced computing power enabled previously unimaginable forms of collecting, storing and sharing of personal data. International core data protection principles were developed, including the obligation to: obtain personal information fairly and lawfully; limit the scope of its use to the originally specified purpose; ensure that the processing is adequate, relevant and not excessive; ensure its accuracy; keep it secure; delete it when it is no longer required; and grant individuals the right to access their information and request corrections.[9] The Human Rights Committee provided clear indications in its general

---

[6] See the Universal Declaration on Human Rights (art. 12); the International Covenant on Civil and Political Rights (ICCPR, art. 17); the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14); and the Convention on the Rights of the Child (art. 16).

[7] See the European Convention for the Protection of Human Rights and Fundamental Freedoms (art. 8) and the Cairo Declaration on Human Rights in Islam (A/45/421-S/21797, art. 18), 5 August 1990.

[8] African Charter on Human and People's Rights (art. 11). See also the African Union's Declaration of Principles on Freedom of Expression in Africa (art. 4.3) and the American Declaration of the Rights and Duties of Man (art. 5).

[9] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72).

comment No. 16 that these principles were encapsulated by the right to privacy,[10] but data protection is also emerging as a distinct human or fundamental right. Some countries have recognized data protection even as a constitutional right, thereby highlighting its importance as an element of democratic societies. The detailed article 35 of the 1976 Constitution of Portugal can be seen as an example of best practice here.

13. The right to privacy is not an absolute right. Once an individual is being formally investigated or screened by a security agency, personal information is shared among security agencies for reasons of countering terrorism and the right to privacy is almost automatically affected. These are situations where States have a legitimate power to limit the right to privacy under international human rights law. However, countering terrorism is not a trump card which automatically legitimates any interference with the right to privacy. Every instance of interference needs to be subject to critical assessment.

B. Permissible limitations to the right to privacy

14. Article 17 of the International Covenant on Civil and Political Rights is the most important legally binding treaty provision on the human right to privacy at the universal level. The Covenant has been ratified by 165 States and signed by another six States.[11] Article 4 of the Covenant allows States parties to derogate from some provisions of the Covenant, including article 17. Derogations can be made only during a state of emergency threatening the life of the nation and they are subject to several conditions.[12] During the more than 30 years since the entry into force of the Covenant in 1976, fewer than 10 States parties have introduced a state of emergency with reference to acts, or the threat of, terrorism.[13] Four of them have in

---

[10] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

[11] As of 16 November 2009. The six countries whose signature has not yet been followed by ratification are China, Cuba, Guinea-Bissau, Nauru, Panama and San Marino.

[12] For the position of the pertinent treaty monitoring body in respect of the scope and effect of derogations, see Human Rights Committee, general comment No. 29 (2001).

[13] Azerbaijan, Chile, Colombia, El Salvador, Israel, Nepal, Peru, the Russian Federation and the United Kingdom.

that context sought to derogate also from article 17 of the Covenant.[14] Another eight States have announced derogation from article 17 without an explicit reference to terrorism as the cause for a state of emergency.[15] However, the notifications in question have remained rather generic, instead of specifying, in line with the requirements under article 4, what concrete measures derogating from article 17 are necessary within the exigencies of the situation.[16] Overall, there is not a single case of a State seeking to derogate from article 17 with reference to terrorism that would demonstrate compliance with all requirements of article 4. Further, only one State has announced derogation from the Covenant with reference to the current (related to the events of 11 September 2001) threat of international terrorism.[17] The situation is similar in respect of reservations to article 17. Although international law generally allows for reservations by States to human rights treaties, provided such reservations are not incompatible with the object and purpose of the treaty,[18] only one State party has submitted a reservation to article 17.[19]

15. Consequently, it appears that States have only rarely resorted to the acknowledged mechanisms available under international law in general, and the Covenant in particular, for unilateral exceptions to the right to privacy. Even when notifications of derogation from article 17 have been submitted, those notifications have remained generic, instead of referring to

---

[14] Colombia, El Salvador, Nepal and the Russian Federation.

[15] Algeria, Armenia, Ecuador, Nicaragua, Panama, Serbia and Montenegro, Sri Lanka and the Bolivarian Republic of Venezuela. In some of these cases, there may have been a factual link to terrorism, although this was not mentioned in the notification concerning a state of emergency.

[16] For instance, when seeking to derogate from ICCPR, many Latin American States have plainly notified that some named provisions of the Covenant will be "suspended". This is not in line with the requirements of art. 4 as explained in general comment No. 29.

[17] The United Kingdom on 18 December 2001. The derogations did not include art. 17 and were withdrawn on 15 March 2005.

[18] For the position of the pertinent treaty monitoring body in respect of reservations to the ICCPR and its optional protocols, see Human Rights Committee, general comment No. 24 (2004).

[19] Liechtenstein maintains a reservation concerning the scope of the right to respect for family life with regard to foreigners.

practical measures and specific forms of derogation. To the Special Rapporteur, the State practice reported above demonstrates that, generally, States appear to be content that the framework of article 17 is flexible enough to enable necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations, including when responding to terrorism. The Special Rapporteur supports this view. Article 17 is written in a manner that allows States parties the possibility to introduce restrictions or limitations in respect of the rights enshrined in that provision, including the right to privacy. Such restrictions and limitations will therefore be subject to the monitoring functions of the Human Rights Committee as the treaty body entrusted with the task of interpreting the provisions of the Covenant and addressing the conduct of States parties in respect of their treaty obligations. The main mechanisms for the exercise of those functions are the mandatory reporting procedure under article 40 of the Covenant and, for those 113 States that have ratified the First Optional Protocol to the Covenant, the procedure for individual complaints.

16. The wording of article 17 of the Covenant prohibits "arbitrary or unlawful" interference with privacy, family or correspondence, as well as "unlawful attacks" on a person's honour and reputation. This can be contrasted with the formulation of such provisions as article 12, paragraph 3; article 18, paragraph 3; article 19, paragraph 3; article 21 and article 22, paragraph 2, which all spell out the elements of a test for permissible limitations. In its most elaborate form, this test is expressed in article 21 and article 22, paragraph 3, as consisting of the following three elements: (a) restrictions must be prescribed by national law; (b) they must be necessary in a democratic society; and (c) they must serve of one of the legitimate aims enumerated in each of the provisions that contain a limitations clause.

17. The Special Rapporteur takes the view that, despite the differences in wording, article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17. Consequently, limitations to the right to privacy or other dimensions of article 17 are subject to a permissible limitations test, as set forth by the Human Rights Committee in its general comment No. 27

(1999). That general comment addresses freedom of movement (art. 12), one of the provisions that contains a limitations clause. At the same time, it codifies the position of the Human Rights Committee in the matter of permissible limitations to the rights provided under the Covenant. The permissible limitations test, as expressed in the general comment, includes, inter alia, the following elements:

(a) Any restrictions must be provided by the law (paras. 11-12).

(b) The essence of a human right is not subject to restrictions (para. 13).

(c) Restrictions must be necessary in a democratic society (para. 11).

(d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13).

(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14).

(f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14-15).

(g) Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18).[20]

18. The Special Rapporteur takes the view that these considerations apply also in respect of article 17 of the Covenant, as elaborations of the notions of "unlawful" and "arbitrary". Where the textual difference between article 17 and the Covenant provisions that explicitly introduce a limitations test nevertheless matters is in the absence of an exhaustive list of legitimate aims in article 17. Here, the Special Rapporteur calls upon States to justify why a particular aim is legitimate as justification for restrictions upon article 17, and upon the Human Rights Committee to continue monitoring measures undertaken by States parties, including through the consideration of periodic reports and of individual complaints.

[20] See Human Rights Committee, general comment No. 27 (1999).

19. In the view of the Special Rapporteur, the Human Rights Committee should draw up and adopt a new general comment on article 17, replacing current general comment No. 16 (1988). The existing general comment is very brief and does not reflect the bulk of the Committee's practice that has emerged during the more than 20 years since its adoption. Nevertheless, many of the elements for a proper limitations clause, presented above in the light of the subsequent general comment No. 27, were already present in 1988.[21] In its subsequent case law under the Optional Protocol, the Committee has emphasized that interference with the rights guaranteed in article 17 must cumulatively meet several conditions, i.e., it must be provided for by law, be in accordance with the provisions, aims and objectives of the Covenant, and be reasonable in the particular circumstances of the case.[22] Further, in finding violations of article 17, the Committee has applied the requirements of legitimate aim, necessity and proportionality.[23]

C. Erosion of the right to privacy by counter-terrorism policies

20. When considering current counter-terrorism policies, States often contend that there are two new dynamics that must be considered alongside privacy protection. First, States claim that their ability to prevent and investigate terrorist acts is linked intimately with increased surveillance powers. The majority of counter-terrorism legislation activities since the events of 11 September 2001 have therefore focused on expanding Governments' powers to conduct surveillance. Second, States claim that since terrorism is a global activity, the search for terrorists must also take place beyond national borders, with the help of third parties which potentially hold extensive amounts of information on individuals, generating a rich resource for identifying and monitoring terrorist suspects. States that previously lacked constitutional or statutory safeguards have been able to radically transform their surveillance powers with few restrictions. In countries that have constitutional and legal safeguards, Governments have

---

[21] See Human Rights Committee, general comment No. 16 (1988). See, in particular, paras. 3 and 4 that elaborate upon the notions of arbitrary and unlawful interference in ICCPR, art. 17.

[22] See *Van Hulst v. The Netherlands*, communication No. 903/1999, 2004.

[23] See *Madafferi v. Australia*, communication No. 1011/2001, 2004, and *M.G. v. Germany*, communication No. 1482/2006, 2008.

endangered the protection of the right to privacy by not extending these safeguards to their cooperation with third countries and private actors, or by placing surveillance systems beyond the jurisdiction of their constitutions.

1. Increasing surveillance measures

21. The range of surveillance operations runs from the specific to the general. At the specific level, legal systems are capable of authorizing and overseeing: undercover operations and covert surveillance to identify illegal conduct; the accumulation of intelligence on specific individuals to identify breaches of law; and targeted surveillance of individuals to build a legal case. The Special Rapporteur had earlier specified that States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[24] Worldwide, there has been a rise in communications surveillance through the interception of communications by intelligence and law enforcement agencies. There is a remarkable convergence in the types of policies pursued to enhance surveillance powers to respond to terrorism threats. Most of these policies rely upon existing or new technologies, such as "bugs" and tracing technologies that can access the geographical position of mobile phones, technology that reports to Governments the contents of private text conversations of users of voice over Internet protocol,[25] or that installs spyware on suspects' computers in order to enable remote computer access.[26] In some countries, security services have even proposed banning communication technologies that are more

[24] A/HRC/10/3, para. 30.

[25] D. O'Brien, "Chinese Skype client hands confidential communications to eavesdroppers", Electronic Frontier Foundation, 2 October 2008.

[26] See the article at the following address: http://www.bundestag.de/dokumente/textarchiv/2008/22719940_kw46_bka/index.html

difficult to intercept, such as smartphones.[27] The Special Rapporteur is also concerned about the tracking of cross-border communications without judicial authorization.[28]

22. In the name of countering terrorism, States have expanded initiatives to identify, scan, and tag the general public through the use of multiple techniques which might violate an individual person's right to privacy. When surveillance occurs of places and larger groups of people, the surveillance is typically subject to weaker regimes for authorisation and oversight. Human rights standards have been tested, stretched and breached through the use of stop-and-searches; the compilation of lists and databases; the increased surveillance of financial, communications and travel data; the use of profiling to identify potential suspects; and the accumulation of ever larger databases to calculate the probability of suspicious activities and identify individuals seen as worthy of further scrutiny. More advanced techniques are applied, as well, such as the collection of biometrics or the use of body scanners that can see through clothing.[29] Some intrusions into people's lives can be permanent as people's physical and biographical details are frequently centralized in databases.

(a) Stop and search powers

23. States have expanded their powers to stop, question, search, and identify individuals, and have reduced their controls to prevent abuse of these powers. These powers have given rise to concerns regarding racial profiling and discrimination in Europe[30] and the Russian Federation[31] and concerns that these powers antagonize the relationship between citizens and the State. Equally, the proportionality requirement in the limitations test to the right to privacy

---

[27] S. Das Gupta and L. D'Monte, "BlackBerry security issue makes e-com insecure", *Business Standard*, 12 March 2008.

[28] See, for instance, the Swedish Government's bill on adjusted defence intelligence operations, adopted in June 2008, p. 83.

[29] See the European Parliament resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection.

[30] Open Society Justice Initiative, *Ethnic Profiling by Police in Europe*, June 2005.

[31] Open Society Justice Initiative and JURIX, *Ethnic Profiling in the Moscow Metro*, June 2006.

raises questions whether blanket stop and search powers in designated security zones, such as in the Russian Federation[32] or the United Kingdom,[33] are really necessary in a democratic society.

(b) The use of biometrics and dangers of centralized identity systems

24. A key component to new identity policies is the use of biometric techniques, such as facial recognition, fingerprinting, and iris-scanning. While these techniques can, in some circumstances, be a legitimate tool for the identification of terrorist suspects, the Special Rapporteur is particularly concerned about cases where biometrics are not stored in an identity document, but in a central database, thereby increasing the information security risks and leaving individuals vulnerable. As the collection of biometric information increases, error rates may rise significantly.[34] This may result in the wrongful criminalization of individuals or social exclusion. Meanwhile, unlike other identifiers, biometrics cannot be revoked: once copied and/or fraudulently used by a malicious party, it is not possible to issue an individual with a new biometric signature.[35] In this context, it has to be noted that, contrary to its scientific objectivity, DNA evidence can also be falsified.[36]

25. Centralized collection of biometrics creates a risk of causing miscarriages of justice, which is illustrated by the following example. Following the Madrid bombings of 11 March 2004, the Spanish police managed to lift a fingerprint from an unexploded bomb. Fingerprint experts from the United States Federal Bureau of Investigation (FBI) declared that a lawyer's fingerprint was a match to the crime-scene sample. The person's fingerprint was on the

---

[32] 2006 Federal Act No. 35 on Counteraction of Terrorism.

[33] See, e.g., United Kingdom Appeal Court, *R. v. Commissioner of Police for the Metropolis and another*, 2006.

[34] See, for example, M. Cherry and E. Imwinkelried, "A cautionary note about fingerprint analysis and reliance on digital technology", *Judicature*, vol. 89, No. 6 (2006).

[35] See E. Kosta et al., "An analysis of security and privacy issues relating to RFID enabled ePassports", International Federation for Information Processing, No. 232 (2007), pp. 467-472.

[36] See, for example, D. Frumkin et al., "Authentification of forensic DNA samples" *Forensic Science International: Genetics* (17 July 2009).

national fingerprint system because he was a former soldier of the United States. The individual was detained for two weeks in solitary confinement, even though the fingerprint was not his. Examiners failed to sufficiently reconsider the match, a situation that was made worse for him when it was discovered that he, as a lawyer, had defended a convicted terrorist, was married to an Egyptian immigrant, and had himself converted to Islam.[37]

(c) The circulation of secret watch lists

26. Another available technique is watch-list monitoring. The most common type of watch-list monitoring is the "no-fly/selectee" list. Such lists are circulated to airlines and security officials with instructions to detain and question any passenger with a certain name. Little is known of the extent to which these lists are being used, but where these systems are publicly overseen, a number of errors and privacy concerns have arisen, particularly in the United States[38] and Canada.[39] Data integrity issues remain, as the lists have to be continually checked for errors and the identification processes must be performed with great care. These lists are frequently kept secret as they could tip off suspected terrorists, but at the same time this secrecy gives rise to problems of individuals being continually subject to scrutiny without knowing that they are on some form of list, and without effective independent oversight. Such secret surveillance could constitute a violation of the right to privacy under article 17 of the International Covenant on Civil and Political Rights.

27. Where terrorist lists have been made public, article 17 of the Covenant is triggered in another form. The Human Rights Committee has concluded that the unjustified inclusion of a person on the United Nations 1267 Committee's Consolidated List constituted a violation of article 17. It considered that the dissemination of personal information constituted an attack on

---

[37] See the United States Department of Justice, Office of the Inspector General, *A Review of the FBI's Handling of the Brandon Mayfield Case*, January 2006.

[38] See the United States Department of Justice, *Audit of the FBI Terrorist Watchlist Nomination Practices*, May 2009.

[39] See the Office of the Privacy Commissioner Canada, *Audit of the Passenger Protect Program of Transport Canada*, November 2009

the honor and reputation of the listed persons, in view of the negative association that would be made between the names and the title of the sanctions list.[40]

28. Public and secret watch lists often also breach fundamental principles of data protection. Information generated for one purpose is reused for secondary purposes, and sometimes shared with other institutions, without the knowledge or consent of the individuals concerned. Erroneous information is used to make decisions about people, which result in restrictions on travel. These individuals may be refused a visa, turned away at a border or prevented from boarding a plane, without having been presented with evidence of any wrongdoing.

(d) Checkpoints and borders

29. Through the use of new technologies and in response to rising concerns regarding terrorism, States are increasing the monitoring, regulation, interference and control of the movement of people at borders. Now, with the use of more advanced technologies and data-sharing agreements, States are creating comprehensive profiles on foreign travellers to identify terrorists and criminals even in advance of their arrival at borders, by accessing passenger manifests and passenger reservation records from carriers. States analyse this information to identify patterns that correspond to those of terrorists or criminals. At the border, individuals are subjected to further – potentially invasive – information collection practices.

30. Many States now require carriers to submit passenger manifests prior to departure. States are also seeking access to passenger name records, which include identification information (name, telephone number), transactional information (dates of reservations, travel agent, itineraries), flight and seat information, financial data (credit card number, invoice address), choice of meals and information regarding place of residence, medical data, prior travel information, and frequent-flyer information. This information is used for profiling and risk-assessing passengers, usually by submitting queries to various multi-agency law enforcement and terrorist databases and watch lists. As a result, foreign carriers may be

[40] See Human Rights Committee, communication No. 1472/2006, paras. 10.12-10.13.

restricted from issuing an individual with a boarding pass solely on the basis of the results of a database query in the destination country, without due process.

31. The increased monitoring of immigrants and travellers for various purposes gives rise to a number of privacy challenges. States are gaining information on travellers from third parties who are compelled to comply lest they be refused landing rights or given punitive fines, even though privacy guarantees may not meet the requirements of domestic privacy laws. Moreover, foreigners might not be granted equal access to judicial remedies in these countries and rights at borders are usually significantly restricted. The United States Government policy on access to travellers' laptops is a useful example. Despite the need to meet constitutional due process requirements for searching a laptop within the United States, the Department of Homeland Security has approved the accessing of travellers' computers without judicial authorisation.[41]

32. Lastly, States are establishing additional information requirements. Individuals can be prevented from entering States for refusing to disclose information, and States may insist upon disclosure without ensuring that there is lawful authority to require this information. Additionally, information collected for one purpose is now being used for additional purposes; for example, the European Union's European Dactyloscopie system (EURODAC) for managing applications of asylum-seekers and illegal immigrants through the use of fingerprints is now proposed to be extended to aid the prevention, detection, and investigation of terrorist offences and other serious offences. The European Data Protection Supervisor has expressed doubts as to whether these proposals are legitimate under the right to privacy.[42]

2. How surveillance has affected other rights

33. Surveillance regimes adopted as anti-terrorism measures have had a profound, chilling effect on other fundamental human rights. In addition to constituting a right in itself, privacy

[41] See the Department of Homeland Security, *Privacy impact assessment for the border searches of electronic devices*, 25 August, 2009.

[42] See the statement by the European Data Protection Supervisor on law enforcement access to EURODAC, 8 October 2009.

serves as a basis for other rights and without which the other rights would not be effectively enjoyed. Privacy is necessary to create zones to allow individuals and groups to be able to think and develop ideas and relationships. Other rights such as freedom of expression, association, and movement all require privacy to be able to develop effectively. Surveillance has also resulted in miscarriages of justice, leading to failures of due process and wrongful arrest.

34. In many nations around the world, users are being monitored to review what sites they are visiting and with whom they are communicating. In Germany, the Federal Intelligence Service was found in 2006 to have been illegally spying on journalists using communications surveillance and placing spies in newsrooms.[43] In Colombia, the Administrative Department of Security was found, in 2009, to have been conducting illegal surveillance of members of the media, human rights workers, Government officials and judges, and their families for seven years.[44] In numerous countries across the world, internet users must show identification and their sessions are recorded for future use by authorities. For instance, in Internet service providers in Bangladesh were required in 2007 to turn over records of their users' identities, passwords and usage to the authorities. Some users were then visited by the authorities, who searched though their computers and contact lists.[45] In the United States, the FBI counter-terrorism unit monitored the activities of peace activists at the time of the 2004 political conventions.[46] These surveillance measures have a chilling effect on users, who are afraid to visit websites, express their opinions or communicate with other persons for fear that they will face sanctions.[47] This is especially relevant for individuals wishing to dissent and might deter

[43] Deutsche Welle World, "Germany stops journalist spying in wake of scandal", 15 May 2006.

[44] See *Semana*, 21 February 2009.

[45] See *E-Bangladeshi*, "Crackdown on internet users in Bangladesh", 3 October 2007 (translating BBC reports).

[46] See the American Civil Liberties Union, "ACLU uncovers FBI Surveillance of main peace activists", 25 October 2006.

[47] See D. S. Sidhu, "The chilling effect of government surveillance programs on the use of the Internet by Muslim-Americans", *University of Maryland Law Journal of Race, Religion, Gender and Class*, vol. 7 (2007), p. 375.

some of these persons from exercising their democratic right to protest against Government policy.

35. In addition to surveillance powers, many anti-terrorism laws require individuals to proactively disclose information and provide broad powers for officials to demand information for investigations. In this context, the Special Rapporteur has earlier expressed his concerns about the use of national security letters in the United States.[48] Some countries have expanded this power to require the disclosure of information originally collected for journalistic purposes. In Uganda, the 2002 Anti-Terrorism Act allows for wiretapping and searches of the media if there are "special reasonable grounds" that the information has "substantial value" in an anti-terrorism investigation.[49] The Special Rapporteur stresses that the legitimate interest in the disclosure of confidential materials of journalists outweighs the public interest in the non-disclosure only where an overriding need for disclosure is proved, the circumstances are of a sufficiently vital and serious nature and the necessity of the disclosure is identified as responding to a pressing social need.[50]

36. The rights to freedom of association and assembly are also threatened by the use of surveillance. These freedoms often require private meetings and communications to allow people to organize in the face of Governments or other powerful actors. Expanded surveillance powers have sometimes led to a "function creep", when police or intelligence agencies have labelled other groups as terrorists in order to allow the use of surveillance powers which were given only for the fight against terrorism. In the United States, environmental and other peaceful protestors were placed on terrorist watch lists by the Maryland State Police before political conventions in New York and Denver.[51] In the United Kingdom, surveillance cameras

---

[48] A/HRC/6/17/Add.3, para. 51.

[49] Anti-terrorism Act, third schedule, para. 8.

[50] See also recommendation No. R (2000) 7, of the Council of Europe Committee of Ministers to member States on the right of journalists not to disclose their sources of information and Ontario Superior Court of Justice, *O'Neill v. Canada (Attorney General)*, 2006, para. 163.

[51] See L. Rein and J. White, "More groups than thought monitored in police spying", *The Washington Post*, 4 January 2009.

are commonly used for political protests and images kept in a database.[52] A recent poll in the United Kingdom found that one third of individuals were disinclined to participate in protests because of concern about their privacy.[53]

37. Freedom of movement can also be substantially affected by surveillance. The creation of secret watch lists, excessive data collection and sharing and imposition of intrusive scanning devices or biometrics, all create extra barriers to mobility. As described in previous sections, there has been a substantial increase in the collection of information about people travelling both nationally and internationally. Information is routinely shared and used to develop watch lists that have led to new barriers to travel. When profiles and watch lists are developed using information from a variety of sources with varying reliability, individuals may have no knowledge of the source of the information, may not question the veracity of this information, and have no right to contest any conclusions drawn by foreign authorities. A mosaic of data assembled from multiple databases may cause data-mining algorithms to identify innocent people as threats.[54] If persons are prohibited from leaving a country, the State must provide information on the reasons requiring the restriction on freedom of movement. Otherwise, the State is likely to violate article 12 of the International Covenant on Civil and Political Rights.[55]

38. One of the most serious effects of surveillance measures is that they may lead to miscarriages of justice and violate due process guarantees. The challenge of gaining access to judicial review is that some legal regimes may prevent access to the courts unless individuals can show that interference has taken place, which is precluded by the secretive nature of the surveillance programmes. Individuals may not be able to prove or demonstrate that they are

---

[52] See P. Lewis and M. Vallée, "Revealed: police databank on thousands of protesters", *The Guardian*, 6 March 2009.

[53] See A. Jha and J. Randerson, "Poll shows public disquiet about policing at environmental protests", *The Guardian*, 25 August 2009.

[54] See United States National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals*, October 2008.

[55] See, similarly, Human Rights Committee, *B. Zoolfia v. Uzbekistan*, communication No. 1585/2007, 2009, para. 8.3.

actually under surveillance. As a result, individuals may not be able to appeal to courts for remedy. In relevant cases, courts have ruled that individuals lack standing because they cannot demonstrate that they were under surveillance and any injuries have been considered speculative.[56] In other cases, where interference can be proven, States have sometimes applied the "State secrets" privilege to avoid scrutiny of illegal surveillance projects.[57] The Special Rapporteur commends the approach of the European Court of Human Rights (ECHR) where individuals do not need to prove that such measures necessarily had applied to them.[58]

3. Extending legal boundaries

39. Mutual legal assistance treaties are established to permit countries to cooperate in investigations and to share information in specific cases.[59] Agreements have also been established to permit the sharing of information on individuals engaged in activities, e.g., all passengers travelling to another country or all individuals conducting interbank financial transactions. More opaque are the agreements between intelligence agencies to share databases and intelligence data. These databases are often subject to wide-ranging exemptions from the domestic legal system. Even if domestic legislation applies, the data may refer to foreign nationals who may not be permitted to exercise any rights in domestic courts. Individuals may not be aware of the fact that they are subject to surveillance – e.g., that they are on a list of suspected terrorists – because intelligence-driven lists are not publicly available and therefore they may not appeal for review. When that list is shared internationally individuals may not be able to identify why they were first placed on it, or otherwise be able to remove themselves from the multiplicity of lists that have emerged since then.

---

[56] This was most recently concluded in *Amnesty International et al. v. John McConnell et al.*, United States District Court for the Southern District of New York, 20 August 2009.

[57] See United States District Court for the Northern District of California, *Al-Haramain Islamic Foundation et al. v. Bush et al.*, 1 May 2009.

[58] See ECHR, *Klass v. Germany*, 6 September 1978, para. 38.

[59] See G. Hosein, *International Co-operation as a Promise and a Threat, in Cybercrime and Jurisdiction: A Global Survey* (T.M.C. Asser Press), 2006.

40. States have increased not only their cooperation with each other in the fight against terrorism, but also with private third parties that have personal information of individuals in order to identify and monitor terrorist suspects. Some Governments have subsequently endangered the protection of the right to privacy by not extending domestic privacy safeguards to their cooperation with third countries and private actors.

41. Third parties, such as banks, telephone companies or even cybercafes, now hold extensive personal information about individuals. Access to this information therefore provides significant details about the private lives of individuals. At the same time, Government agencies may gain access to this information with fewer restrictions than if the information was held by individuals themselves, in the home, or even by other Government agencies. In the United States, for instance the Supreme Court has ruled that, as data provided to third parties such as banks or telephone companies is shared "freely" with these parties, individuals may not reasonably expect privacy.[60] Where there is a lack of constitutional protections that require a legal basis for the interference in the private lives of individuals, the burden then falls on the private organization to decide how to respond to a request from a Government agency. Generally, the private sector prefers that Governments establish a legal basis for obliging organizations to produce personal information upon request, as it removes their obligation to consider the nature of the case.

42. Third parties are also increasingly being called upon to collect more information than is necessary, and to retain this information for extended periods of time. The United Kingdom, for instance, has proposed that telecommunications companies actively monitor and retain information on individuals' online activities including social-networking activities – information that these companies have no justified interest in collecting.[61] Similarly, the

---

[60] See United States Supreme Court, *Smith v. Maryland*, 1979, in the case of communications data, and *United States v. Miller*, 1976, in the case of financial information.

[61] See British All Party Parliamentary Group on Privacy, *Briefing Paper: Inquiry into communications data surveillance proposals and the Interception Modernisation Programme*, June 2009.

European Union's data retention directive[62] has generated considerable criticism. When, in 2008, the German Federal Constitutional Court temporarily suspended the German law implementing that directive, it noted that "the retention of sensitive data, comprehensive and without occasion, on virtually everyone, for Government purposes that at the time of the storage of the data cannot be foreseen in detail, may have a considerable intimidating effect."[63] Also in Germany, research showed a chilling effect of data retention policies: 52 per cent of persons interviewed said they probably would not use telecommunication for contact with drug counsellors, psychotherapists or marriage counsellors because of data retention laws.[64]

43. In this context, the Special Rapporteur is concerned that, in many countries, data retention laws have been adopted without any legal safeguards over the access to this information being established or without the fact that new technological developments are blurring the difference between content and communications data being considered. While constitutional provisions tend to require safeguards on access to communications content, the protection of transaction logs is more limited. While this information may be integral to investigations, it may also be just as privacy-sensitive as the content of communications transactions.

44. With the goal of combating terrorism financing and money laundering, States have obliged the financial industry to analyse financial transactions in order to automatically distinguish those "normal" from those "suspicious". For instance, the European Union established a directive in 2005 on "the prevention of the use of the financial system for the

---

[62] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal*, L 105(2006), pp. 54-63.

[63] Constitutional Court decision No. 256/08, 11 March 2008.

[64] German Forsa Institute, *Meinungen der Bunderburger zur Vorratsdatanspeicherung*, 28 May 2008.

purpose of money laundering and terrorist financing"[65] requiring that financial institutions follow due diligence by reporting suspicious and "threshold" activities to financial intelligence units (FIUs). The additional processing of this information by the FIUs remains opaque, but States like Australia[66] and Canada[67] are processing millions of transactions each year through advanced data-mining tools.

45. Third parties may also be subject to foreign laws requiring disclosure. The United States Government, for instance, issued administrative subpoenas to the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the Belgian cooperative responsible for enabling messaging between more than 7,800 financial institutions in over 200 countries. By gaining access to the SWIFT data centre in the United States, the country's Treasury was then able to monitor foreign financial transactions across the SWIFT network, to find and identify terrorist suspects.[68] Human rights groups filed legal complaints in over 20 courts arguing that, by handing this information over to United States authorities, SWIFT was in breach of local privacy laws.[69]

46. The Special Rapporteur is also concerned that surveillance is being embedded in technological infrastructures, and that these will create risks for individuals and organizations. For example, the development of standards for lawful interception of communications requires telecommunications companies to design vulnerabilities into their technologies to ensure that States may intercept communications. These capabilities were abused in Greece where unknown third parties were able to listen to the communications of the Prime Minister of

---

[65] See Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, *Official Journal,* L 309 (.2005), pp. 15-36.

[66] See Australian Transaction Reports and Analysis Centre, *AUSTRAC Annual Report 2008-09*, October 2009.

[67] See Financial Transaction and Reports Analysis Centre of Canada, *FINTRAC Annual Report 2008*, 11 September 2008.

[68] See also the statement of United States Under Secretary Stuart Levey on the Terrorist Finance Tracking Program, 23 June 2006.

[69] See, for example, Privacy International, "Pulling a Swift one? Bank transfer information sent to U.S. authorities", 27 July 2006.

Greece, and dozens of other high-ranking dignitaries.[70] More recently, these same capabilities were reported to have been used by the Government of the Islamic Republic of Iran to monitor protestors.[71] To avoid abuse, surveillance technologies should log who accesses data, thereby leaving a trail that can itself be monitored for abuse.[72]

47. In some States, constitutional safeguards continue to apply, however. In Canada, for example, the Charter of Rights and Freedoms protects privacy of information held by third parties when it reveals "intimate details of the lifestyle and personal choices of the individual".[73] This requires balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.[74] The jurisprudence of the European Convention of Human Rights has similarly extended the right to privacy to information held by third parties. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data requires both the public and private sectors to protect the information that they hold and regulates the sharing of information with Government agencies. Exceptions apply when protecting State security, public safety or the monetary interests of the State, suppressing criminal offences or protecting individuals or the rights and freedoms of others.[75]

D. Best practices

48. The Special Rapporteur is concerned that there is a trend towards extending such State surveillance powers beyond terrorism. Following the events of 11 September 2001, a number of legislatures introduced sunset clauses into and reviews of anti-terrorism legislation, as it was

---

[70] See, for background, V. Prevelakis and D. Spinellis, "The Athens Affair", *IEEE Spectrum*, July 2007.

[71] See, for reference, Nokia Siemens Networks, "Provision of lawful intercept capability in Iran", 22 June 2009.

[72] See footnote 54.

[73] See Supreme Court of Canada, *R. v. Plant*, 1993, and *R. v. Tessling*, 2004.

[74] *R. v. Plant*.

[75] Art. 9 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

assumed that extraordinary powers may be required for a short period of time to respond to the then danger. These sunset clauses and reviews were not included in some areas of policymaking and, in later policies, were not considered at all. Many of the investigative powers given to law enforcement agencies under anti-terror laws are granted to these agencies to conduct investigations unrelated to terrorism. Meanwhile, States are following each other's lead on policy without considering the human rights implications. Many of the policies outlined above were introduced first as extraordinary, but then soon became regional and international standards. Collectively, such interference is having significant negative impacts on the protection of the right to privacy, as there is limited access to legal safeguards. Without a rigorous set of legal safeguards and a means to measure the necessity, proportionality, or reasonableness of the interference, States have no guidance on minimizing the risks to privacy generated by their new policies. The Special Rapporteur has identified the legal safeguards that have emerged through policymaking, jurisprudence, policy reviews and good practice from around the world.

1. The principle of minimal intrusiveness

49. Some interference with the private lives of individuals is more intrusive than others. Constitutional protection of property and people has been extended over the past 50 years to include communications,[76] information that is related to a biographical core[77] and a right to the confidentiality and integrity of information-technological systems.[78] These protections require States to have exhausted less-intrusive techniques before resorting to others. The United Kingdom Parliament's Home Affairs Committee reviewed and adapted these ideas for modern data-centred surveillance systems into the principle of data-minimization, which is closely linked to purpose-specification.[79] In its review, the Parliamentary committee recommended that Governments "resist a tendency to collect more personal information and establish larger databases. Any decision to create a major new database, to share information on databases, or

[76] See United States Supreme Court, *Katz v. United States*, 1967.

[77] See footnote 74.

[78] See German Constitutional Court decision No. 370/07, 27 February 2008.

[79] See the United Kingdom Parliament's Home Affairs Committee, *A Surveillance Society? Fifth report of the session 2007-2008*, 8 June 2008.

to implement proposals for increased surveillance, should be based on a proven need." The Special Rapporteur contends that States must incorporate this principle into existing and future policies as they present how their policies are necessary, and in turn proportionate.

2. The principle of purpose specification restricting secondary use

50. Whereas data protection law should protect information collected for one purpose being used for another, national security and law enforcement policies are generally exempted from these restrictions. This is done through secrecy provisions in lawful access notices, broad subpoenas and exemption certificates such as national security certificates, which exempt a specific database from adhering to privacy laws. The Special Rapporteur is concerned that this limits the effectiveness of necessary safeguards against abuse. States must be obliged to provide a legal basis for the reuse of information, in accordance with constitutional and human rights principles. This must be done within the human rights framework, rather than resorting to derogations and exemptions. This is particularly important when information is shared across borders; furthermore, when information is shared between States, protections and safeguards must continue to apply.[80]

3. The principle of oversight and regulated authorization of lawful access

51. Surveillance systems require effective oversight to minimize harm and abuses. Where safeguards exist, this has traditionally taken the form of an independent authorization through a judicial warrant and/or a subpoena process with the opportunity of independent review. Many policies have attempted to restrict oversight and lower authorization levels, however: communications interception laws have minimized authorization requirements for some communications; secret subpoenas are issued to gain access to information held by third parties and have restricted the ability to seek judicial protections; and States are increasingly allowing intelligence and law enforcement agencies to self-authorize access to personal information

[80] See, for instance, with regard to passenger name records, the Article 29 Data Protection Working Party's opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America, 30 September 2004.

where previously some form of independent authorization and effective reporting was necessary.

52. Some States have taken measures to address the erosion of safeguards. In the United States, after a number of court cases and because of the reauthorization requirements under the USA Patriot Act, more opportunities for judicial review have been reintroduced. Changes to the communications surveillance practices in Sweden and the United States have reintroduced some limited safeguards in the form of judicial warrants. Similarly, the European Court of Justice ruled that courts had to review the domestic lawfulness of international watch lists.[81]

53. The Special Rapporteur is concerned that the lack of effective and independent scrutiny of surveillance practices and techniques calls into question whether interferences are lawful (and thus accountable) and necessary (and thus applied proportionately). He commends the hard work of oversight bodies within Government agencies, including internal privacy offices, audit departments and inspectorate-generals, as they too play a key role in identifying abuses. The Special Rapporteur therefore calls for increased internal oversight to complement the processes for independent authorization and external oversight. This internal and external accountability system will ensure that there are effective remedies for individuals, with meaningful access to redress mechanisms.

4. The principle of transparency and integrity

54. The application of secrecy privileges for surveillance systems inhibits the ability of legislatures, judicial bodies and the public to scrutinize State powers. Individuals may be subject to inappropriate surveillance, where profiles are developed through data mining, and erroneous judgements, without any prior notification of the practice. Furthermore, the lack of clear and appropriate limitations to surveillance policies makes it difficult to prove that these powers are not use in arbitrary and indiscriminate manners.

---

[81] *Yassin Abdullah Kadi and Al Barakaat International Foundation v. Council and Commission*, September 2008.

55. The principle of transparency and integrity requires openness and communication about surveillance practices. In some States, individuals must be notified when and how they are under surveillance, or as soon as possible after the fact. Under *habeas data* constitutional regimes in Latin America[82] and European data protection laws, individuals must be able to gain access to and correct their personal information held within data stores and surveillance systems. These rights must be ensured across borders by ensuring that legal regimes protect citizens and non-citizens alike.

56. Open debate and scrutiny is essential to understanding the advantages and limitations of surveillance techniques, so that the public may develop an understanding of the necessity and lawfulness of surveillance. In many States, parliaments and independent bodies have been charged with conducting reviews of surveillance policies and procedures, and on occasion have been offered the opportunity for pre-legislative review. This has been aided by the use of sunset and review clauses in legislation.

5. The principle of effective modernization

57. Even as more invasive information is available with greater ease, States have not developed commensurate protection. In fact, in the name of modernizing their surveillance powers, States sometimes have intentionally sought to apply older and weaker safeguard regimes to ever more sensitive information.[83] Conscious of the need to consider how technology and policy change may have a negative impact on individuals, some States have introduced privacy impact assessments that articulate privacy considerations in the design of new surveillance techniques, including how policymakers considered many of the principles listed above, including data minimization and rights to redress. The Special Rapporteur believes that the use of such tools as privacy impact assessments may help inform the public about surveillance practices, while instilling a culture of privacy within Government agencies

---

[82] See, e.g., Constitution of Brazil, art. 5 (LXXI); Constitution of Paraguay, art. 135; Constitution of Argentina, art. 43.

[83] See the Policy Engagement Network, *Briefing on the UK Government's Interception Modernisation Programme*, June 2009.

as they develop new surveillance systems to combat terrorism. International standards must also be adopted to require States to enhance their safeguards to reflect technological change.

IV. CONCLUSIONS AND RECOMMENDATIONS

A. Conclusions

58. **The Special Rapporteur is concerned that what was once exceptional is now customary. First, States no longer limit exceptional surveillance schemes to combating terrorism and instead make these surveillance powers available for all purposes. Second, surveillance is now engrained in policymaking. Critics of unwarranted surveillance proposals must now argue why additional information must not be collected, rather than the burden of proof residing with the State to argue why the interference is necessary. Third, the quality and effectiveness of nearly all legal protections and safeguards are reduced. This is occurring even as technological change allows for greater and more pervasive surveillance powers. Most worrying, however, is that these technologies and policies are being exported to other countries and often lose even the most basic protections in the process.**

59. **International legal standards must be developed to ensure against these forms of abuse. This would be aided by adherence to principles outlined in this report, including ensuring that surveillance is as unintrusive as possible and that new powers are developed with appropriate safeguards and limitations, effective oversight and authorization and regular reporting and review and are accompanied by comprehensive statements regarding the impact on privacy. The general public and legislatures have rarely had the opportunity to debate whether anti-terrorism powers are necessary, proportionate or reasonable. The Special Rapporteur believes that following emergent good practices may prove beneficial to all.**

B. Recommendations

For legislative assemblies

60. **The Special Rapporteur recommends again that any interference with the right to privacy, family, home or correspondence should be authorized by provisions of law that are publicly accessible, particularly precise and proportionate to the security threat, and offer effective guarantees against abuse. States should ensure that the competent authorities apply less intrusive investigation methods if such methods enable a terrorist offence to be detected, prevented or prosecuted with adequate effectiveness. Decision-making authority should be structured so that the greater the invasion of privacy, the higher the level of authorization needed.**

61. **Adherence to international standards for privacy and human rights protection must be a tenet national law. Accordingly, a comprehensive data protection and privacy law is necessary to ensure that there are clear legal protections for individuals to prevent the excessive collection of personal information, that ensures measures are in place to ensure the accuracy of information, that creates limits on the use, storage, and sharing of the information, and which mandates that individuals are notified of how their information is used and that they have a right to access and redress, regardless of nationality and jurisdiction.**

62. **Strong independent oversight mandates must be established to review policies and practices, in order to ensure that there is strong oversight of the use of intrusive surveillance techniques and the processing of personal information. Therefore, there must be no secret surveillance system that is not under the review of an effective oversight body and all interferences must be authorized through an independent body.**

63. **All current and proposed counter-terrorism policies must include privacy impact assessments to review and communicate how the policy and technologies ensure that privacy risks are mitigated and privacy is considered at the earliest stages of policymaking.**

64. **The Special Rapporteur recommends that stronger safeguards be developed to ensure that the sharing of information between governments continues to protect the privacy of individuals.**

65. **The Special Rapporteur also recommends that stronger regulations are developed to limit Government access to information held by third parties, including reporting schemes, and to minimizes the burden placed on third parties to collect additional information, and that constitutional and legal safeguards apply when third parties are acting on behalf of the State.**

66. **The Special Rapporteur warns that legislative language should be reconsidered to prevent the use of anti-terrorism powers for other purposes. New systems must be designed with a limitation of scope in the specifications.**

For Governments

67. **The Special Rapporteur urges Governments to articulate in detail how their surveillance policies uphold the principles of proportionality and necessity, in accordance with international human rights standards, and what measures have been taken to ensure against abuse.**

68. **The Special Rapporteur recommends open discussion and regular reporting on information-based surveillance programmes. Reports to legislative and oversight bodies, as well as independent reviews of practices will help inform future policymaking and deliberation on anti-terrorism policy.**

69. **Any watch list- or profile-based surveillance programme must include due process safeguards for all individuals, including rights to redress. The principle of transparency must be upheld so that individuals can be informed as to why and how they were added to watch lists or how their profile was developed, and of the mechanisms for appeal without undue burdens.**

70. **Given the inherent dangers of data mining, the Special Rapporteur recommends that any information-based counter-terrorism programme should be subjected to robust and independent oversight. The Special Rapporteur also recommends against the development and use of data-mining techniques for counter-terrorism purposes.**

71. **In light of the risk of abuse of surveillance technologies, the Special Rapporteur recommends that equal amounts of research and development resources be devoted to privacy-enhancing technologies.**

For the Human Rights Council

72. **The Special Rapporteur recommends the development of a programme for global capacity-building on privacy protection. The international replication of anti-terrorism laws and the global standards on surveillance must be counterbalanced with greater awareness of the necessary safeguards for the protection of individuals' dignity.**

73. **The Special Rapporteur urges the Human Rights Council to establish a process that builds on existing principles of data protection to recommend measures for the creation of a global declaration on data protection and data privacy.**

For the Human Rights Committee

74. **The Special Rapporteur recommends that the Human Rights Committee begins drafting a new general comment on article 17 of the International Covenant on Civil and Political Rights, with the goal of elaborating a proper limitation test, thereby providing guidance to States on appropriate safeguards. The general comment should also give due attention to data protection as an attribute of the right to privacy, as enshrined in article 17 of the Covenant**.

- - - - -