PRIVACY INTERNATIONAL

Guide to International Law and Surveillance

Privacy International

August 2017

Guide to International Law and Surveillance

The 21st century has brought with it rapid development in the technological capacities of Governments and corporate entities to intercept, extract, filter, store, analyse, and disseminate the communications of whole populations. The costs of retaining data have decreased drastically, and continue to do so every year, and the means of analysing the information have improved exponentially due to developments in automated machine learning and algorithmic designs. These technological advancements have rendered the safeguards protecting the right to privacy obsolete. Recent revelations about the scope and nature of mass surveillance and bulk interception programs have led to a surge in legal discourse surrounding the role that international law, and in particular international human rights law, can and should play in responding to this evolving reality.

International and regional courts, international human rights treaty bodies, U.N. agencies, multilateral organizations, and special rapporteurs, have all published authoritative statements on the law surrounding the right to privacy in the sphere of surveillance. The "Guide to International Law and Surveillance" is an attempt to collate relevant excerpts from these judgments and reports into a single principled guide that will be continuously updated. Despite its name the guide isn't just aimed at lawyers. It is really a handy reference tool for anyone engaging in campaigning, advocacy, and scholarly research, on these issues.

The guide is quite long but there is no need to read it cover to cover. We suggest that you either use the hyperlinked table of contents or search for key words to find the most relevant quotes from you. The guide is thus meant to be used in a light touch way, but providing you with the most hard-hitting results.

The guide covers array of relevant topics such as the (il)legality of mass surveillance operations, the law surrounding data retention, the extraterritorial application of human rights law and digital surveillance, the international law on hacking for surveillance purposes, crypto-wars and the "going dark" debate, and the responsibility of multinational corporations in protecting the right to privacy.

The first section of the guide offers an abridged version, a compressed list of the most substantive articulations of law surrounding of the sub-issues covered, as they are reflected under both U.N. law and Regional Human Rights Law. If you cite nothing else, these are the quotes that you want to reference. The second section of the guide offers additional quotes for each of the sub-issues, beyond the primary ones introduced in the first section.

The guide is a living and breathing document and we will be adding new content as more statements and resolutions emerge. Please reach out to us via Twitter (@Privacyint) if you have any other quotes you want us to add or topics you want us to cover.

Table of Contents

A. Highlighted Quotes

B. Additional Quotes

Chapter 1: The Right to Privacy in International and Regional Treaties

Universal Declaration of Human Rights, Article 12 (10 December 1948)

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

American Declaration on the Rights and Duties of Man, Article V: Right to protection of honor, personal reputation, and private and family life (2 May 1948)

"Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life."

European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8: Right to Respect for Private and Family Life (4 November 1950)

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

International Covenant on Civil and Political Rights, Article 17 (16 December 1966)

"1. 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.

2. Everyone has the right to the protection of the law against such interference or attacks."

American Convention on Human Rights (Pact of San Jose), Article 11: Right to Privacy (22 November 1969)

"1. Everyone has the right to have his honor respected and his dignity recognized.

2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.

3. Everyone has the right to the protection of the law against such interference or attacks."

Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Part 1: General (23 September 1980)

"2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties...

6. These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data."

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 1: Object and Purpose (28 January 1981)

"The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."

Convention on the Rights of the Child, Article 16 (20 November 1989)

"1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation.

2. The child has the right to the protection of the law against such interference or attacks."

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 14 (18 December 1990)

"No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks."

Charter of Fundamental Rights of the European Union, Article 7: Respect for Private and Family Life, and Article 8: Protection of Personal Data (7 December 2000)

"7. Everyone has the right to respect for his or her private and family life, home and communications.

8. (1) Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; (3) Compliance with these rules shall be subject to control by an independent authority."

The Arab Charter on Human Rights, Article 16 and Article 21 (22 May 2004)

"16. Everyone charged with a criminal offence shall be presumed innocent until proved guilty by a final judgment rendered according to law and, in the course of the investigation and trial, he shall enjoy the following minimum guarantees: … (8) The right to respect for his security of person and his privacy in all circumstances.

21. (1) No one shall be subjected to arbitrary or unlawful interference with regard to his privacy, family, home or correspondence, nor to unlawful attacks on his honour or his

reputation; (2) Everyone has the right to the protection of the law against such interference or attacks."

Convention on the Rights of Persons with Disabilities, Article 22: Respect for Privacy (13 December 2006)

"1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.

2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others."

Chapter 2A: Principles Surrounding Surveillance and the Right to Privacy

A. The Principle of Legality

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

"*Noting* in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must undertake the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"153. ...the limitations on [the right to privacy and associated rights] must be established beforehand in a law, and set forth expressly, exhaustively, precisely, and clearly, both substantively and procedurally. This means that there must be a law that results from the deliberation of a legislative body, which precisely defines the causes and conditions that would enable the State to intercept the communications of individuals, collect communications data or "metadata," or to subject them to surveillance or monitoring that invades spheres in which they have reasonable expectations of privacy."

154. As this Office of the Special Rapporteur has already indicated, clandestine espionage conducted unlawfully or without legal support is an act that is highly offensive to fundamental rights and seriously compromises the actions of the State, its international responsibility, and even the very basis of democracy."

Taylor-Sabori v. The United Kingdom, App. No. 47114/99, European Court of Human Rights, Judgment (22 October 2002)

"18. The Court notes that it is not disputed that the surveillance carried out by the police in the present case amounted to an interference with the applicant's rights under Article 8 § 1 of the Convention. It recalls that the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of covert surveillance by public authorities, in this instance the police, domestic law must provide protection against arbitrary interference with an individual's right under Article 8. Moreover, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures.

19. At the time of the events in the present case there existed no statutory system to regulate the interception of pager messages transmitted via a private telecommunication system. It follows, as indeed the Government have accepted, that the interference was not "in accordance with the law". There has, accordingly, been a violation of Article 8."

i. Accessibility Requirement

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"29. ...[S]ecret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion... The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight. Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights.

Malone v. The United Kingdom, App. No. 8691/79, European Court of Human Rights, Judgment (2 August 1984)

"70. The issue to be determined is therefore whether, under domestic law, the essential elements of the power to intercept communications were laid down with reasonable precision in accessible legal rules that sufficiently indicated the scope and manner of exercise of the discretion conferred on the relevant authorities...

79. ...in its present state the law in England and Wales governing interception of communications for police purposes is somewhat obscure and open to differing interpretations... on the evidence before the Court, it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive. In view of the attendant obscurity and uncertainty as to the state of the law in this essential respect, the Court cannot but reach a similar conclusion to that of the Commission. In the opinion of the Court, the law of England and Wales does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking."

ii. Foreseeability Requirement

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015)

"24. The State party should: ...(b) Ensure that any interference with the right to privacy with the family, with the home or with correspondence is authorized by laws that (i) are publicly accessible; (ii) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under

surveillance, the limit on the duration of surveillance, and procedures for the use and storage of data collected; and (iv) provide for effective safeguard against abuse."

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

"93. As to the third requirement, the law's foreseeability, the Court reiterates that foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures.

94. Moreover, since the implementation in practice of measures of secret surveillance of communication is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred to the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."

B. The Principle of Necessity

John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, Brief of Amici Curiae, United Nations Human Rights Experts in Support of Plaintiff-Appellant and Reversal, D.C. Ct. App., Case No. 16-7081, pp. 14-15, 17-18 (1 November 2016)

"It is also unlikely that Ethiopia's surveillance activities are "necessary" for the protection of the objectives specified under Article 19(3). The requirement of necessity implies that restrictions must not simply be useful, reasonable or desirable to achieve a legitimate government objective. Instead, a State must demonstrate "in specific and individualized fashion the precise nature of the threat" that it seeks to address, and a "direct and immediate connection between the expression and the threat." Necessity also implies an assessment of proportionality of the relevant restrictions. In particular, States must show that the restrictions are appropriate to achieve their protective function … the least intrusive instrument amongst those which might achieve their protection function … [and] proportionate to the interest to be protected."

Ethiopia's alleged surveillance of Kidane is neither necessary nor proportionate. As a threshold matter, the U.N. Human Rights Committee... has found that "the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights" is never a legitimate objective; in fact, it undermines public engagement and debate in a manner that runs counter to the letter of Article 19 and the object and purposes of the Covenant. Accordingly, Ethiopia cannot justify surveillance activities as necessary if it targeted Kidane merely because of his human rights work. In any case, the continuous, real-time interception and collection of Kidane's digital

communications and activities for almost five months is unlikely to be proportionate to any legitimate interest Ethiopia's seeks to achieve...

The indiscriminate recording and monitoring of Kidane's private digital life for four and a half months is also "arbitrary." At a minimum, an interference with privacy is "arbitrary" if it is unpredictable, capricious and unreasonable. Arbitrariness "is not confined to procedural arbitrariness, but extends to the reasonableness of the interference with the person's rights under Article 17 and its compatibility with the purposes, aims and objectives of the Covenant." A number of international bodies and experts – including the Human Rights Committee, the U.N. High Commisioner for Human Rights, and various U.N. Special Rapporteurs – conclude that an interference with privacy in non-arbitrary only if it is necessary to achieve a legitimate aim, [and] proportionate to the aim sought.

There is no evidence that Ethiopia has met any of these criteria. It allegedly intercepted and collected Kidane's private communications and personal data and those of his family without asserting any public justification, and without any evident effort to minimize the information collected. Moreover, Ethiopia only attempted to cease its surveillance activities after they were exposed by The Citizen Lab at the University of Toronto, in March 2013."

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

"104. The Court shares the Government's view that the aim of the impugned provisions of the amended G10 Act was indeed to safeguard national security and/or to prevent crime, which are legitimate aims within the meaning of Article 8 § 2. It does not, therefore, deem it necessary to decide whether the further purposes cited by the Government were also relevant.

105. It remains to be ascertained whether the impugned interferences were "necessary in a democratic society" in order to achieve these aims.

106. The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interferences with an applicant's right to respect for his or her private life, it has consistently recognized that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aims of protecting national security. Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law."

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

"71. ...the mere requirement for the authorities to give reasons for the request, arguing for the necessity of secret surveillance, falls short of an assessment of strict necessity. There is no legal safeguard requiring TEK to produce supportive materials or, in particular, a sufficient factual basis for the application of secret intelligence gathering measures which would enable the evaluation of necessity of the proposed measure - and this on the basis of an individual

suspicion regarding the target person. For the Court, only such information would allow the authorising authority to perform an appropriate proportionality test.

72. Quite apart from what transpires from section 53(2) of the National Security Act, the Court recalls at this point that in Klass and Others it held that "powers of secret surveillance of citizens ... are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions". Admittedly, the expression "strictly necessary" represents at first glance a test different from the one prescribed by the wording of paragraph 2 of Article 8, that is, "necessary in a democratic society".

73. However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity – an approach it considers convenient to endorse."

C. The Principle of Proportionality

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"51. It is incumbent upon States to demonstrate that any interference with the right to privacy under article 17 of the Covenant is a necessary means to achieving a legitimate aim. This requires that there must be a rational connection between the means employed and the aim sought to be achieved. It also requires that the measure chosen be "the least intrusive instrument among those which might achieve the desired result". The related principle of proportionality involves balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest. However, there are limits to the extent of permissible interference with a Covenant right. As the Human Rights Committee has emphasized, "in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right". In the context of covert surveillance, the Committee has therefore stressed that any decision to allow interference with communications must be taken by the authority designated by law "on a case-by-case basis". The proportionality of any interference with the right to privacy should therefore be judged on the particular circumstances of the individual case."

Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)

"46. In that regard, according to the settled case-law of the Court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the

legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.

47. With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference.

48. In the present case, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict."

D. The Principle of Adequate Safeguards

U.N. Human Rights, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (8 April 1988)

"10. ...Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant."

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

"95. In the case-law on secret measures of surveillance the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."

Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015)

"233. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust

supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure.

234. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications."

i. Reasonable Suspicion

Concluding Observations on the Fourth Periodic Report of the Republic of Korea, Human Rights Committee, U.N. Doc. CCPR/C/KOR/CO/4 (3 December 2015)

"42. The Committee notes with concern that, under article 83 (3) of the Telecommunications Business Act, subscriber information may be requested without a warrant by any telecommunications operator for investigatory purposes…

43. The State party should introduce the legal amendments necessary to ensure that any surveillance, including for the purposes of State security, is compatible with the Covenant. It should, inter alia, ensure that subscriber information may be issued with a warrant only."

Klass and Others v. Germany, App. No. 5029/71, European Court of Human Rights, Judgment (6 September 1978)

"51. According to the G 10, a series of limitative conditions have to be satisfied before a surveillance measure can be imposed. Thus, the permissible restrictive measures are confined to cases in which there are factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts; measures may only be ordered if the establishment of the facts by another method is without prospects of success or considerably more difficult; even then, the surveillance may cover only the specific suspect or his presumed "contact-persons". Consequently, so-called exploratory or general surveillance is not permitted by the contested legislation. Surveillance may be ordered only on written application giving reasons, and such an application may be made only by the head, or his substitute, of certain services; the decision thereon must be taken by a Federal Minister empowered for the purpose by the Chancellor or, where appropriate, by the supreme Land authority. Accordingly, under the law there exists an administrative procedure designed to ensure that measures are not ordered haphazardly, irregularly or without due and proper consideration. In addition, although not required by the Act, the competent Minister in practice and except in urgent cases seeks the prior consent of the G 10 Commission."

ii. Effective Oversight

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

"4. *Calls upon all States*... (*d*) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data..."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"45. One of the core protections afforded by article 17 is that covert surveillance systems must be attended by adequate procedural safeguards to protect against abuse. These safeguards may take a variety of forms, but generally include independent prior authorization and/or subsequent independent review. Best practice requires the involvement of the executive, the legislature and the judiciary, as well as independent civilian oversight...

46. Where targeted surveillance programmes are in operation, many States make provision for prior judicial authorization. Judicial involvement that meets international standards is an important safeguard, although there is evidence that in some jurisdictions the degree and effectiveness of such scrutiny has been circumscribed by judicial deference to the executive...

47. In the context of targeted surveillance, whichever method of prior authorization is adopted (judicial or executive), there is at least an opportunity for ex ante review of the necessity and proportionality of a measure of intrusive surveillance by reference to the particular circumstances of the case and the individual or organization whose communications are to be intercepted. Neither of these opportunities exists in the context of mass surveillance schemes since they do not depend on individual suspicion. Ex ante review is thus limited to authorizing the continuation of the scheme as a whole, rather than its application to a particular individual...

61. States should establish strong and independent oversight bodies that are adequately resourced and mandated to conduct ex ante review, considering applications for authorization not only against the requirements of domestic law, but also against the necessity and proportionality requirements of the Covenant. In addition, individuals should have the right to seek an effective remedy for any alleged violation of their online privacy rights. This requires a means by which affected individuals can submit a complaint to an independent mechanism that is capable of conducting a thorough and impartial review, with access to all relevant material and attended by adequate due process guarantees. Accountability mechanisms can take a variety of forms, but must have the power to order a binding remedy."

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, European Court of Human Rights, Judgment (28 June 2007)

"85. Unlike the system of secret surveillance under consideration in the case of Klass and Others, the SSMA does not provide for any review of the implementation of secret surveillance measures by a body or official that is either external to the services deploying the means of surveillance or at least required to have certain qualifications ensuring his independence and adherence to the rule of law. Under the SSMA, no one outside the services actually deploying special means of surveillance verifies such matters as whether these services in fact comply with the warrants authorising the use of such means, or whether they faithfully reproduce the original data in the written record. Similarly, there exists no independent review of whether the original data is in fact destroyed within the legal ten-day time-limit if the surveillance has

proved fruitless. On the contrary, it seems that all these activities are carried out solely by officers of the Ministry of Internal Affairs. It is true that the Code of 1974 provided, in its Article 111b § 6, that the judge who had issued a surveillance warrant had to be informed when the use of special means of surveillance has ended. So does Article 175 § 6 of the Code of 2005. It is also true that there is an obligation under section 19 of the SSMA to inform the issuing judge when the use of special means of surveillance has been discontinued before the end of the authorised period. However, the texts make no provision for acquainting the judge with the results of the surveillance and do not command him or her to review whether the requirements of the law have been complied with. Moreover, it appears that the provisions of the Codes of 1974 and 2005 are applicable only in the context of pending criminal proceedings and do not cover all situations envisaged by the SSMA, such as the use of special means of surveillance to protect national security...

87. The Court further notes that the overall control over the system of secret surveillance is entrusted solely to the Minister of Internal Affairs – who not only is a political appointee and a member of the executive, but is directly involved in the commissioning of special means of surveillance –, not to independent bodies, such as a special board elected by the Parliament and an independent commission, as was the case in Klass and Others, or a special commissioner holding or qualified to hold high judicial office, as was the case in Christie, or a control committee consisting of persons having qualifications equivalent to those of a Supreme Court judge, as was the case in L. v. Norway. A dissenting judge in the Constitutional Court had serious misgivings about this complete lack of external control.

88. Moreover, the manner in which the Minister effects this control is not set out in the law. Neither the SSMA, nor any other statute lays down a procedure governing the Minister's actions in this respect. The Minister has not issued any publicly available regulations or instructions on the subject. Moreover, neither the Minister, nor any other official is required to regularly report to an independent body or to the general public on the overall operation of the system or on the measures applied in individual cases."

iii. Data Retention

Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014)

"Refrain from imposing mandatory retention of data by third parties."

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"26. Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of Governments on private sector actors to retain data "just in case" it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.

34. ...where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert

jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty."

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015)

"55. Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information."

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

"132. The Court notes in the first place that the impugned provisions, in providing for the destruction of personal data as soon as they were no longer needed to achieve their statutory purpose, and for the verification at regular, fairly short intervals of whether the conditions for such destruction were met, constituted an important element in reducing the effects of the interference with the secrecy of telecommunications to an unavoidable minimum."

Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016)

"77. The protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies.

85. The principle of confidentiality of communications established by Directive 2002/58 implies, inter alia, as stated in the second sentence of Article 5(1) of that directive, that, as a general rule, any person other than the users is prohibited from storing, without the consent of the users concerned, the traffic data related to electronic communications. The only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication...

86. Accordingly, as confirmed by recitals 22 and 26 of Directive 2002/58, under Article 6 of that directive, the processing and storage of traffic data are permitted only to the extent necessary and for the time necessary for the billing and marketing of services and the provision of value added services. As regards, in particular, the billing of services, that processing is permitted only up to the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that period has elapsed, the data processed and stored must be erased or made anonymous. As regards location data other than traffic data, Article 9(1) of that directive provides that that data may be processed only subject to certain conditions and after it has been made anonymous or the consent of the users or subscribers obtained.

87. The scope of Article 5, Article 6 and Article 9(1) of Directive 2002/58, which seek to ensure the confidentiality of communications and related data, and to minimise the risks of misuse, must moreover be assessed in the light of recital 30 of that directive, which states: 'Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum'...

103. ...while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight...

105. National legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy...

109. In order to satisfy the requirements set out in the preceding paragraph of the present judgment, that national legislation must, first, lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary.

110. Second, as regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.

111. As regard the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the

basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.

122. With respect to the rules relating to the security and protection of data retained by providers of electronic communications services... providers [are required] to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period."

iv. Transparency Requirements

Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7 (28 April 2016)

"36. While acknowledging the number of safeguards in place to prevent abuse in the application of the Signals Intelligence Act, the Committee remains concerned about the limited degree of transparency with regard to the scope of such surveillance powers and the safeguards on their application...

37. The State party should increase the transparency of the powers of and safeguards on the National Defence Radio Establishment, the Foreign Intelligence Court and the Data Inspection Board, by considering to make their policy guidelines and decisions public, in full or in part, subject to national security considerations and the privacy interests of individuals concerned by those decisions..."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"166. The State must be transparent with respect to the laws regulating communications surveillance and the criteria used for their application. The principle of "maximum disclosure" is applicable to this issue, and indeed governs all State acts: they are public and can only be kept secret from the public under the strictest circumstances, provided that this confidentiality is established by law, seeks to fulfil a legitimate aim under the American Convention, and is necessary in a democratic society.

167. As the European Court of Human Rights has held, a secret surveillance system can "undermine or even destroy democracy under the cloak of defending it." The Court therefore demands that there be "adequate and effective guarantees against abuse." To determine whether this is being done in a particular case, the Court indicated that it is necessary to examine "nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law."

168. States should disclose general information on the number of requests for interception and surveillance that have been approved and rejected, and should include as much information as possible, such as—for example—a breakdown of requests by service provider, type of investigation, time period covered by the investigations, etc.

169. The service providers should be able to publicly disclose the procedures they use when they receive requests for information from government authorities, as well as information on at least the types of requests they receive and the number of requests. On this point, it bears noting that various internet companies have adopted the practice of issuing transparency reports that disclose some aspects of the government requests for access to user information they receive."

v. Safeguards in Intelligence Sharing and Data Transfers

Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7 (28 April 2016)

"36. [The Committee is] concerned about the lack of sufficient safeguards against arbitrary interference with the right to privacy with regard to the sharing of raw data with other intelligence agencies.

37. The State party should increase the transparency of the powers of and safeguards on the National Defence Radio Establishment, the Foreign Intelligence Court and the Data Inspection Board, by considering to make their policy guidelines and decisions public, in full or in part, subject to national security considerations and the privacy interests of individuals concerned by those decisions. It should ensure: (a) that all laws and policies regulating the intelligence-sharing of personal data are in full conformity with its obligations under the Covenant, in particular article 17, including the principles of legality, proportionality and necessity; (b) that effective and independent oversight mechanisms over intelligence-sharing of personal data are put in place; and (c) that affected persons have proper access to effective remedies in cases of abuse."

European Commission For Democracy Through Law (Venice Commission), Report on the Democratic Oversight of the Security Services, Study No. 388/2006 CDL-AD(2007)016 (11 June 2007)

"115. Treaties on mutual assistance between police, customs and judicial authorities are nowadays an important feature of the fight against transnational organised crime. Similarly, as already mentioned, improved international intelligence cooperation is necessary to combat terrorism in particular. However, this necessary improved cooperation can cause problems as far as concerns accountability for security services. Accountability arrangements tend to track the policies or actions of national security and intelligence agencies. Frequently, the legislation contains either express or implied limitations that inhibit oversight or review of arrangements made with the intelligence agencies of other countries...

117. Concrete examples of abuses involving international exchanges of intelligence are unlikely to come to light, although the recent Maher Arar case is in Canada is an exception. The main obstacles that national accountability bodies face in this task are a combination of "plausible deniability" and lack of powers to supervise such arrangements. Where a security agency merely receives "anonymized" intelligence from an overseas agency with which it has

an arrangement, it can argue that it is not responsible for how the information was obtained. A security agency might accept responsibility in theory where it had actively requesting a foreign agency to obtain information from a suspect by means which are not lawful in the receiving agency's State. The problem will be that this level of involvement can rarely, if ever, be substantiated. The receiving agency will almost invariably be able to argue that it had no knowledge of that illegitimate measures have been used to obtain the intelligence, and no reason to suspect that such measures were used. Allegations of illegal or unethical behaviour can be "plausibly denied" since the receiving agency was not responsible for them. A truthful but incomplete denial can therefore be given to any suggestion that the information was improperly obtained by the receiving agency.

118. Moreover, there can be strong incentives for the receiving agency not to inquire into how information was obtained. An agency in a country with limited foreign intelligence gathering capability may be dependent on friendly foreign agencies providing it with intelligence. If the receiving agency asks too many questions, it may well receive embarrassing answers, namely that the material was indeed obtained by unethical means. One could argue that the receiving agency should try to insist that the supplying agency certifies compliance with human rights standards, but the supplying agency may simply refuse.

119. The exercise of police power is primarily national. That means that whatever national restrictions which apply to obtaining information tend only to apply to actions within the territory or to direct actions by State officials. This leaves the clear possibility that an agency may benefit from intelligence collected overseas by another country's agency through means that it would not be legally permitted to use.

120. In so far as one agency supplies information to another country's agency, again accountability is flawed since the information is unlikely to result in a decision that can be directly traced to the supplying agency. Information may be supplied on terms that the source is not revealed to any other body, including the courts or whatever the oversight bodies exist in the receiving State. Even where this is not so the confidentiality of the source of the information may be protected either under legislation in the receiving country or through the actions of its courts in the name of not harming international relations. Where the legal systems of both the supplying and receiving agencies protect the secrecy of international relations in this way, the result is a vacuum of accountability. The supply of information to multilateral bodies - for example to the UN Sanctions Committee or, for EU States, under the EU Third Pillar bodies, may also suffer from comparable defects of accountability.

121. The case-law of the ECtHR is still developing in the area of the extent to which a State can, and should, bear responsibility for acts with an extraterritorial dimension. It is, however, already evident that a vacuum of accountability is not acceptable."

Draft agreement between Canada and the European Union on the Transfer of Passenger Name Record data (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)

"124. ...the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental right [...], whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities. In this connection, it does not matter

whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference

125. Consequently, both the transfer of PNR data from the European Union to the Canadian Competent Authority and the framework negotiated by the European Union with Canada of the conditions concerning the retention of that data, its use and its subsequent transfer to other Canadian authorities, Europol, Eurojust, judicial or police authorities of the Member States or indeed to authorities of third countries, [...] constitute interferences with the right...

141. In order to satisfy [the principle of proportionality], the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing. Those considerations apply particularly where the protection of the particular category of personal data that is sensitive data is at stake...

168. ...the PNR data transferred to Canada is mainly intended to be subject to analyses by automated means, based on pre-established models and criteria and on cross-checking with various databases.

169. the assessment of the risks to public security presented by air passengers is carried out [...] by means of automated analyses of the PNR data before the arrival of those air passengers in Canada. Since those analyses are carried out on the basis of unverified personal data and are based on pre-established models and criteria, they necessarily present some margin of error, as, inter alia, the French Government and the Commission conceded at the hearing...

171. It is true that, as regards the consequences of the automated processing of PNR data, Article 15 of the envisaged agreement provides that Canada is not to take 'any decisions significantly adversely affecting a passenger solely on the basis of automated processing of PNR data'...

172. That being so, the extent of the interference which automated analyses of PNR data entail in respect of the rights enshrined in Articles 7 and 8 of the Charter essentially depends on the pre-established models and criteria and on the databases on which that type of data processing is based... the pre-established models and criteria should be specific and reliable, making it possible [...] to arrive at results targeting individuals who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime and should be non-discriminatory. Similarly, it should be stated that the databases with which the PNR data is cross-checked must be reliable, up to date and limited to databases used by Canada in relation to the fight against terrorism and serious transnational crime.

173. Furthermore, since the automated analyses of PNR data necessarily involve some margin of error [...] any positive result obtained following the automated processing of that data must [...] be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the air passengers concerned is adopted. Consequently, such a

measure may not [...] be based solely and decisively on the result of automated processing of PNR data.

174. Lastly, in order to ensure that, in practice, the pre-established models and criteria, the use that is made of them and the databases used are not discriminatory and are limited to that which is strictly necessary, the reliability and topicality of those pre-established models and criteria and databases used should, taking account of statistical data and results of international research, be covered by the joint review of the implementation of the envisaged agreement...

214. In this connection, it must be recalled that a transfer of personal data from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union. That same requirement applies in the case of the disclosure of PNR data by Canada to third countries [...] in order to prevent the level of protection provided for in that agreement from being circumvented by transfers of personal data to third countries and to ensure the continuity of the level of protection afforded by EU law...

216. Article 12(3) of the envisaged agreement allows Canada to 'make any disclosure of information subject to reasonable legal requirements and limitations ... with due regard for the legitimate interests of the individual concerned'. However, that agreement does not delimit the nature of the information that may be disclosed, nor the persons to whom such disclosure may be made, nor even the use that is to be made of that information

217. Moreover, the envisaged agreement does not define the terms 'legal requirements and limitations' or the terms 'legitimate interests of the individual concerned', nor does it require that the disclosure of PNR data to an individual be linked to combating terrorism and serious transnational crime or that the disclosure be conditional on the authorisation of a judicial authority or an independent administrative body. In those circumstances, that provision exceeds the limits of what is strictly necessary."

vi. Distinctions in Safeguards Between Metadata and Content and Between GEOINT and SIGINT

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

"*Noting* that while metadata can provide benefits, certain types of metadata, when aggregated, can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity."

Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016)

"99. That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means... of establishing a profile of the individuals

concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.

100. The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance.

101. Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights, the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter."

vii. Distinctions in Safeguards Between Law Enforcement and Intelligence Agencies

Liberty and Others v. The United Kingdom, App. No. 58243/00, European Court of Human Rights, Judgment (1 July 2008)

"63. It is true that the above requirements were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses (the equivalent, within the United Kingdom, of the section 3(1) regime). However, the Weber and Saravia case was itself concerned with generalised "strategic monitoring", rather than the monitoring of individuals. The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other..."

viii. Professional Confidentiality and Privileged Communications

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015)

59. States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.

Kopp v. Switzerland, App. No. 23224/94, European Court of Human Rights, Judgment (25 March 1998)

"71. ...[The Government] added that Mr Kopp, the husband of a former member of the Federal Council, had not had his telephones tapped in his capacity as a lawyer. In the instant case, in accordance with Swiss telephone-monitoring practice, a specialist Post Office official had listened to the tape in order to identify any conversations relevant to the proceedings in progress, but no recording had been put aside and sent to the Federal Public Prosecutor's Office.

72. The Court, however, is not persuaded by these arguments. Firstly, it is not for the Court to speculate as to the capacity in which Mr Kopp had had his telephones tapped, since he was a lawyer and all his law firm's telephone lines had been monitored. Secondly, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated. In that connection, the Court by no means seeks to minimise the value of some of the safeguards built into the law, such as the requirement at the relevant stage of the proceedings that the prosecuting authorities' telephone-tapping order must be approved by the President of the Indictment Division, who is an independent judge, or the fact that the applicant was officially informed that his telephone calls had been intercepted.

73. However, the Court discerns a contradiction between the clear text of legislation which protects legal professional privilege when a lawyer is being monitored as a third party and the practice followed in the present case. Even though the case-law has established the principle, which is moreover generally accepted, that legal professional privilege covers only the relationship between a lawyer and his clients, the law does not clearly state how, under what conditions and by whom the distinction is to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to activity other than that of counsel.

74. Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence.

75. In short, Swiss law, whether written or unwritten, does not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter. Consequently, Mr Kopp, as a lawyer, did not enjoy the minimum degree of protection required by the rule of law in a democratic society. There has therefore been a breach of Article 8."

Sommer v. Germany, App. No. 73607/13, European Court of Human Rights, Judgment (27 April 2017)

"48. ... the Court agrees with the parties and holds that collecting, storing and making available the applicant's professional bank transactions constituted an interference with his right to respect for professional confidentiality and his private life...

52. As regards the protection of the professional confidentiality of lawyers, the Court observes that Article 160a § 4 of the [Code of Criminal Procedure (CCP)] does not require there to be a formal investigation against the lawyer who is affected, but that the prohibition of investigative measures against lawyers under Article 160a §§ (1) to (3) of the CCP can be lifted if certain facts substantiate a suspicion of participation in an offence.

52. he Court considers that Articles 161 and 160a of the CCP are worded in rather general terms. It reiterates that, in the context of covert intelligence-gathering, it is essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures

for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness...

56. ... the Court has previously acknowledged the importance of specific procedural guarantees when it comes to protecting the confidentiality of exchanges between lawyer and client and of legal professional privilege. It has emphasised that, subject to strict supervision, it is possible to impose certain obligations on lawyers concerning their relations with their clients, for example in the event that there is plausible evidence of the lawyer's involvement in a crime and in the context of the fight against money-laundering. The Court has further elaborated that the Convention does not prevent domestic law allowing for searches of a lawyer's offices as long as proper safeguards are provided, for example the presence of a representative (or president) of a bar association.

57. Turning to the facts of the present case, the Court firstly notes the wide scope of the prosecutorial requests for information, which concerned information about all transactions relating to the applicant's professional bank account for a period of over two years, as well as information about further, possibly private, bank accounts of the applicant. It agrees with the applicant that the information submitted by the bank provided the public prosecutor and the police with a complete picture of his professional activity for the time in question, and moreover with information about his clients...The fact that only fifty-three transactions were considered relevant and included in the case file, and that the Regional Court restricted access to the relevant parts of the case file later on, could not redress the already ongoing interference, but only limit it from becoming more serious. In sum, the Court concludes that the requests for information were only limited in relation to the period in question, but otherwise concerned all information concerning the bank account and banking transactions of the applicant...

61. The Court observes that Article 160a of the CCP provides a specific safeguard for lawyers and lawyer-client privilege. However, it also notes that such protection can be suspended under Article 160a § 4 of the CCP if certain facts substantiate a suspicion of participation in an offence. According to the Government, with reference to the discussions during the legislative procedure, Article 160a § 4 of the CCP does not require there to be an official investigation against a lawyer before the protection of the professional confidentiality of lawyers is suspended. According to the national authorities and courts, the transfer of fees from the applicant's client's fiancée to the applicant, and the suspicion that money stemming from illegal activities had been transferred to the fiancée's bank account, sufficiently substantiated a suspicion against the applicant. On the basis of the information and documents provided by the parties, the Court considers that the suspicion against the applicant was rather vague and unspecific.

62. . Lastly, the Court observes that the inspection of the applicant's bank account was not ordered by a judicial authority, and that no "specific procedural guarantees" were applied to protect legal professional privilege. In so far as the Government submitted that the applicant could have the measures reviewed by a court under the analogous application of Article 98 § 2 of the CCP, the Court reiterates that a subsequent judicial review can offer sufficient protection if a review procedure at an earlier stage would jeopardise the purpose of an investigation or surveillance. However, the effectiveness of a subsequent judicial review is inextricably linked to the question of subsequent notification about the surveillance measures. There is, in principle, little scope for recourse to the courts by an individual unless he or she is advised of the measures taken without his or her knowledge and thus able to challenge the legality of such measures retrospectively. In that regard, the Court observes that the public prosecutor asked

the bank not to reveal his information requests to the applicant, that the applicant was not informed about the inspection of his professional bank account by the public prosecutor, and that he only learned of the investigative measures concerning his own bank account from the case file. The Court concludes that, even though there was no legal requirement to notify the applicant, by coincidence he learnt of the investigative measures and had access to a retrospective judicial review of the prosecutorial requests for information.

63. Having regard to the low threshold for inspecting the applicant's bank account, the wide scope of the requests for information, the subsequent disclosure and continuing storage of the applicant's personal information, and the insufficiency of procedural safeguards, the Court concludes that the interference was not proportionate and therefore not "necessary in a democratic society". There has accordingly been a violation of Article 8 of the Convention."

E. The Principle of Access to Remedy: Victimhood, Standing, and Notification

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"40. Effective remedies for violations of privacy through digital surveillance can thus come in a variety of judicial, legislative or administrative forms. Effective remedies typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to effective remedy. States take different approaches to notification: while some require post facto notification of surveillance targets, once investigations have concluded, many regimes do not provide for notification. Some may also formally require such notification in criminal cases; however, in practice, this stricture appears to be regularly ignored. There are also variable approaches at national level to the issue of an individual's standing to bring a judicial challenge. The European Court of Human Rights ruled that, while the existence of a surveillance regime might interfere with privacy, a claim that this created a rights violation was justiciable only where there was a "reasonable likelihood" that a person had actually been subjected to unlawful surveillance.

41. Second, effective remedies will involve prompt, thorough and impartial investigation of alleged violations. This may be provided through the provision of an "independent oversight body [...] governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society." Third, for remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation. Such remedial bodies must have "full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders". Fourth, where human rights violations rise to the level of gross violations, non-judicial remedies will not be adequate, as criminal prosecution will be required."

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, European Court of Human Rights, Judgment (28 June 2007)

"58. ...In all these cases the Court found that to the extent that a law institutes a system of surveillance under which all persons in the country concerned can potentially have their mail and telecommunications monitored, without their ever knowing this unless there has been

either some indiscretion or subsequent notification, it directly affects all users or potential users of the postal and telecommunication services in that country. The Court therefore accepted that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting them, without having to allege that such measures were in fact applied to him or her.

59. In line with its holdings in these cases, the Court finds that the second applicant, being an individual, can claim to be victim, within the meaning of Article 34, on account of the very existence of legislation in Bulgaria permitting secret surveillance. It notes in this connection that the applicants do not contend that measures of surveillance were actually applied to them; it is therefore inappropriate to apply a reasonable-likelihood test to determine whether they may claim to be victims of a violation of their Article 8 rights.

60. As regards the applicant association, the Court notes that it has already held that a legal person is entitled to respect for its "home" within the meaning of Article 8 § 1 of the Convention. The applicant association is therefore, contrary to what the Government suggest, not wholly deprived of the protection of Article 8 by the mere fact that it is a legal person. While it may be open to doubt whether, being such a person, it can have a "private life" within the meaning of that provision, it can be said that its mail and other communications, which are in issue in the present case, are covered by the notion of "correspondence" which applies equally to communications originating from private and business premises. The former Commission has already held, in circumstances identical to those of the present case, that applicants who are legal persons may fear that they are subjected to secret surveillance. It has accordingly accepted that they may claim to be victims...

90. Finally, the Court notes that under Bulgarian law the persons subjected to secret surveillance are not notified of this fact at any point in time and under any circumstances. According to the Court's case-law, the fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased cannot by itself warrant the conclusion that the interference was not justified under the terms of paragraph 2 of Article 8, as it is the very unawareness of the surveillance which ensures its efficacy. However, as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned. Indeed, the German legislation in issue in the cases of Klass and Others and Weber and Saravia, as modified by the German Federal Constitutional Court, did provide for such notification. The position in the Leander case was similar.

91. By contrast, the SSMA does not provide for notification of persons subjected to surreptitious monitoring under any circumstances and at any point in time. On the contrary, section 33 of the SSMA, as construed by the Supreme Administrative Court, expressly prohibits the disclosure of information whether a person has been subjected to surveillance, or even whether warrants have been issued for this purpose. Indeed, such information is considered classified. The result of this is that unless they are subsequently prosecuted on the basis of the material gathered through covert surveillance, or unless there has been a leak of information, the persons concerned cannot learn whether they have ever been monitored and are accordingly unable to seek redress for unlawful interferences with their Article 8 rights. Bulgarian law thus eschews an important safeguard against the improper use of special means of surveillance."

Chapter 3A: Surveillance and Other Human Rights Provisions

A. Surveillance and the Jurisdictional Clause (Extraterritorial Application)

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

"*Deeply concerned* at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights."

Concluding observations on the fifth periodic report of France, Human Rights Committee, U.N. Doc. CCPR/C/FRA/CO/5 (17 August 2015)

"12. ...The State Party should take all necessary steps to guarantee that its surveillance activities within and outside its territory are in conformity with its obligations under the Covenant, in particular, Article 17."

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"34. ...[Digital surveillance] may engage a State's human rights obligations if that surveillance the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country then human rights protections must be extended those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violated another State's sovereignty."

B. Surveillance and the Principle of Non-Discrimination

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015); Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014)

"measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance".

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

35. [there exist] ongoing discussions on whether "foreigners" and "citizens" should have equal access to privacy protections within national security surveillance oversight regimes. Several

legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside, or otherwise provide foreign or external communications with lower levels of protection. If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass "off-shore" at some point) and thus allow them to be collected and retained. The result is significantly weaker – or even non-existent – privacy protection for foreigners and non-citizens, as compared with those of citizens.

36. International human rights law is explicit with regard to the principle of non-discrimination. Article 26 of the International Covenant on Civil and Political Rights provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." These provisions are to be read together with articles 17, which provides that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks", as well as with article 2, paragraph 1..."

Chapter 4A: Mass Surveillance Programs

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

"*Deeply concerned* at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights."

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1 (27 April 2016)

"42. ...The Committee is further concerned at reports of unlawful surveillance practices, including mass interception of communications carried out by the National Communications Centre..."

43. ...The State party should refrain from engaging in mass surveillance of private communications without prior judicial authorization..."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"18. Assuming therefore that there remains a legal right to respect for the privacy of digital communications (and this cannot be disputed (see General Assembly resolution 68/167)), the adoption of mass surveillance technology undoubtedly impinges on the very essence of that right. It is potentially inconsistent with the core principle that States should adopt the least intrusive means available when entrenching on protected human rights; it excludes any individualized proportionality assessment; and it is hedged around by secrecy claims that make any other form of proportionality analysis extremely difficult. The States engaging in mass surveillance have so far failed to provide a detailed and evidence-based public justification for its necessity, and almost no States have enacted explicit domestic legislation to authorize its use. Viewed from the perspective of article 17 of the Covenant, this comes close to derogating from the right to privacy altogether in relation to digital communications. For all these reasons, mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law. In the view of the Special Rapporteur, the very existence of mass surveillance programmes constitutes a potentially disproportionate interference with the right to privacy. Shortly put, it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. The very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis.

52. The technical ability to run vast data collection and analysis programmes undoubtedly offers an additional means by which to pursue counter-terrorism and law enforcement investigations. But an assessment of the proportionality of these programmes must also take account of the collateral damage to collective privacy rights. Mass data collection programmes appear to offend against the requirement that intelligence agencies must select the measure that is least intrusive on human rights (unless relevant States are in a position to demonstrate that nothing less than blanket access to all Internet-based communication is sufficient to protect

against the threat of terrorism and other serious crime). Since there is no opportunity for an individualized proportionality assessment to be undertaken prior to these measures being employed, such programmes also appear to undermine the very essence of the right to privacy. They exclude altogether the "case-by-case" analysis that the Human Rights Committee has regarded as essential, and they may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. The Special Rapporteur, accordingly, concludes that such programmes can be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people in any part of the world...

59. The prevention and suppression of terrorism is a public interest imperative of the highest importance and may in principle form the basis of an arguable justification for mass surveillance of the Internet. However, the technical reach of the programmes currently in operation is so wide that they could be compatible with article 17 of the Covenant only if relevant States are in a position to justify as proportionate the systematic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world. Bulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17. In the absence of a formal derogation from States' obligations under the Covenant, these programmes pose a direct and ongoing challenge to an established norm of international law.

63. The Special Rapporteur calls upon all States that currently operate mass digital surveillance technology to provide a detailed and evidence-based public justification for the systematic interference with the privacy rights of the online community by reference to the requirements of article 17 of the Covenant. States should be transparent about the nature and extent of their Internet penetration, its methodology and its justification, and should provide a detailed public account of the tangible benefits that accrue from its use."

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

"68. For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen, especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. These data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like. Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European

Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information.

69. The Court recalls that in Kennedy, the impugned legislation did not allow for "indiscriminate capturing of vast amounts of communications" which was one of the elements enabling it not to find a violation of Article 8. However, in the present case, the Court considers that, in the absence of specific rules to that effect or any submissions to the contrary, it cannot be ruled out that the broad-based provisions of the National Security Act can be taken to enable so-called strategic, large-scale interception, which is a matter of serious concern."

Chapter 5A: Debates Surrounding Surveillance-Related Capabilities

A. The Debate over Encryption and "Going Dark"

U.N. Human Rights Council Resolution on the Safety of Journalists, U.N. Doc. A/HRC/33/L.6 (26 September 2016)

"13. *Emphasizes* that, in the digital age, encryption and anonymity tools have become vital for many journalists to exercise freely their work and their enjoyment of human rights, in particular their rights to freedom of expression and to privacy, including to secure their communications and to protect the confidentiality of their sources, and calls upon States not to interfere with the use of such technologies, with any restrictions thereon complying with States' obligations under international human rights law."

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015)

"31. Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.

32. First, for a restriction on encryption or anonymity to be "provided for by law", it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the. Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.

33. Second, limitations may only be justified to protect specified interests: rights or reputations of others; national security; public order; public health or morals... No other grounds may justify restrictions on the freedom of expression. Moreover, because legitimate objectives are often cited as a pretext for illegitimate purposes, the restrictions themselves must be applied narrowly.

34. Third, the State must show that any restriction on encryption or anonymity is "necessary" to achieve the legitimate objective. The European Court of Human Rights has concluded appropriately that the word "necessary" in article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms means that the restriction must be something more than "useful," "reasonable" or "desirable". Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals.

35. Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online. A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result". The limitation must target a specific objective and not unduly intrude upon other rights of targeted

persons, and the interference with third parties' rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be "proportionate to the interest to be protected". A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high. Moreover, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, "a detailed and evidence-based public justification" is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression...

45. In a situation where law enforcement or national security arguments may justify requests for access to communications, authorities may see two options: order either decryption of particular communications or, because of a lack of confidence that a targeted party would comply with a decryption order, disclosure of the key necessary for decryption. Targeted decryption orders may be seen as more limited and less likely to raise proportionality concerns than key disclosures, focusing on specific communications rather than an individual's entire set of communications encrypted by a particular key. Key disclosures, by contrast, could expose private data well beyond what is required by the exigencies of a situation. Moreover, key disclosure or decryption orders often force corporations to cooperate with Governments, creating serious challenges that implicate individual users online. Key disclosures exist by law in a number of European countries. In both cases, however, such orders should be based on publicly accessible law, clearly limited in scope, focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight.

59. States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.

60. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. In addition, States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users. Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms). Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals."

B. The Debate over Hacking and Vulnerability Exploitation

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (22 July 2015)

"13. Taking into account existing and emerging threats, risks and vulnerabilities and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting and open, secure, stable, accessible and peaceful ICT environment:

(a) Consistent with the purposes of the United nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security...

(f) States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public...

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

(k) States should not conduct or knowingly support activity to harm the information systems of authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity." appropriate measure."

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6 (28 March 2017)

"36. The Committee is concerned about reports alleging a practice of intercepting personal communications by intelligence agencies and the employment of hacking techniques by them without explicit statutory authorization or clearly defined safeguards from abuse...

37. The State party should review the regime regulating the interception of personal communications, hacking of digital devices and the retention of communications data with a view to ensuring (a) that such activities conform with its obligations under article 17 including with the principles of legality, proportionality and necessity, (b) that robust independent oversight systems over surveillance, interception and hacking, including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were subject to measures of surveillance or hacking"

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (17 April 2013)

"62. ...Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. There are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing. Trojans, for example, not only enable a State to access devices, but also enable them to alter – inadvertently or purposefully – the information contained therein. This threatens not only the right to privacy but also procedural fairness rights with respect to the use of such evidence in legal proceedings."

Chapter 6A: Right to Privacy and the Roles and Responsibilities of MNCs

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/71/199 (19 December 2016)

"Expressing concern that individuals often do not provide their free, explicit, and informed consent to the sale or multiple resale of their personal data, as the collecting, processing and sharing of personal data, including sensitive data, have increased significantly in the digital age...

Noting also the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital age,

Welcoming measures taken by business enterprises, on a voluntary basis, to provide transparency to their users about their policies regarding requests by State authorities for access to user data and information.

Recalling that business enterprises have a responsibility to respect human rights and that States must protect against human rights abuses, including of the right to privacy, within their territory and/or jurisdiction by third parties, including business enterprises, as set out in the Guiding Principles on business and Human rights: Implementing the United Nations "Protect, Respect and Remedy" Framework and in accordance with applicable laws and other international principles."

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6 (28 March 2017)

"36. ...[The Committee is concerned] about allegations that companies based in the State party have been providing on-line surveillance equipment to foreign governments with a record of serious human rights violations and the absence of legal safeguards or oversight mechanisms put in place in relation to such exports (art.17).

37. The State Party should... take measures to ensure that all corporations under its jurisdiction, in particular technology corporations, respect human rights standards when engaging in operations abroad."

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"44. Enterprises that provide content or Internet services, or supply the technology and equipment that make digital communications possible, for example, should adopt an explicit policy statement outlining their commitment to respect human rights throughout the company's activities. They should also have in place appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact. Companies should assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users.

45. Where enterprises are faced with government demands for access to data that do not comply with international human rights standards, they are expected to seek to honour the principles of human rights to the greatest extent possible, and to be able to demonstrate their ongoing

efforts to do so. This can mean interpreting government demands as narrowly as possible, seeking clarification from a Government with regard to the scope and legal foundation for the demand, requiring a court order before meeting government requests for data, and communicating transparently with users about risks and compliance with government demands. There are positive examples of industry action in this regard, both by individual enterprises and through multi-stakeholder initiatives.

46. A central part of human rights due diligence as defined by the Guiding Principles is meaningful consultation with affected stakeholders. In the context of information and communications technology companies, this also includes ensuring that users have meaningful transparency about how their data are being gathered, stored, used and potentially shared with others, so that they are able to raise concerns and make informed decisions. The Guiding Principles clarify that, where enterprises identify that they have caused or contributed to an adverse human rights impact, they have a responsibility to ensure remediation by providing remedy directly or cooperating with legitimate remedy processes. To enable remediation at the earliest possible stage, enterprises should establish operational-level grievance mechanisms."

Chapter 2B: Principles Surrounding Surveillance and the Right to Privacy

A. The Principle of Legality (extended)

U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/28/L.27 (24 March 2015)

"*Recognizing* the need to further discuss and analyse, on the basis of international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness and lawfulness, and the relevance of necessity and proportionality assessments in relation to surveillance practices...

Noting that the rapid pace of technological development enables individuals all over the world to use new information and communications technology and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the right to privacy, as set out in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and its therefore an issue of increasing concern."

U.N. Human Rights, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (8 April 1988)

"10. The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."

U.N. Human Rights Committee, Antonius Cornelis Van Hulst v. Netherlands, Comm. No. 903/1999, U.N. Doc. CCPR/C/82/D903/1999 (15 November 2004)

"7.3 The Committee recalls that, in order to be permissible under article 17, any interference with the right to privacy must cumulatively meet several conditions set out in paragraph 1, 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."

Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, Human Rights Committee, U.N. Doc. CCPR/C/MKD/CO/3 (17 August 2015)

"23. The State party should take all measures necessary to ensure that its surveillance activities conform to its obligations under the Covenant, including article 17. In particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity."

Concluding observations on the fifth periodic report of France, Human Rights Committee, U.N. Doc. CCPR/C/FRA/CO/5 (17 August 2015)

"12. ...Specifically, measures should be taken to guarantee that any interference in persons' private lives should be in conformity with the principles of legality, proportionality and necessity. The State party should ensure that the collection and use of data on communications take place on the basis of specific and legitimate objectives and that the exact circumstances in which such interference may be authorized and the categories of persons likely to be placed under surveillance are set out in detail."

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1 (27 April 2016)

"42. The Committee is concerned about the relatively low threshold for conducting surveillance in the State party and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the 2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act...

43. The State party should take all measures necessary to ensure that its surveillance activities conform to its obligations under the Covenant, including article 17, and that any interference with the right to privacy complies with the principles of legality, necessity and proportionality... It should also ensure that interception of communications by law enforcement and security services is carried out only according to the law and under judicial supervision. The State party should increase the transparency of its surveillance policy and speedily establish independent oversight mechanisms to prevent abuses and ensure that individuals have access to effective remedies."

Concluding Observations on the Seventh Periodic Report of Colombia, Human Rights Committee, U.N. Doc. CCPR/AZE/CO/4 (4 November 2016) (as translated from the original Spanish)

"32. ... the Committee is concerned that the inclusion of "monitoring the electromagnetic spectrum" in Article 17 of Law 1621 of 2013 could lead to interferences with private communications made through the electromagnetic spectrum that are not subject to strict assessment of legality, necessity and proportionality. It is also concerned that the new Police Code, which comes into force in January 2017, provides a very broad definition of what is public space, which includes the electromagnetic spectrum, and that all information and data collected in public spaces are subjected to public and free access by the Police.

33. The State Party should: ...(b) Take steps to ensure that any interference with the right to private life, including those that might take place under the monitoring of the electromagnetic spectrum, complies with the principles of legality, necessity and proportionality measures; (d) Ensure that the application of the legislation governing issues that may have consequences for the enjoyment of the right to privacy, in particular Act 1621 and the new Police Code, is entirely consistent with the obligations under the Covenant, in particular Article 17."

Concluding Observations on the Sixth Periodic Report of Morocco, Human Rights Committee, U.N. Doc. CCPR/C/MAR/CO/6 (4 November 2016) (as translated from the original French)

"37. The Committee is concerned at reports of unlawful violations of the right to privacy during surveillance activities by police and intelligence services in particular against journalists, human rights defenders, and those perceived to be opposed to the government, particularly in

Western Sahara. The Committee is also concerned about the lack of clarity on legal provisions that authorize and regulate the activities of surveillance, and lack of oversight over such activities by an independent authority (art. 17).

38. The State party should take all necessary steps to ensure that its monitoring activities are consistent with the Covenant obligations, including Article 17, and ensure that any interference with privacy complies with the principles of legality, proportionality and necessity. It should also establish independent monitoring mechanisms to prevent abuse."

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, U.N. Doc. CCPR/C/POL/CO/7 (4 November 2016)

"39. The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities as reflected in the Law on Counterterrorism of June 2016 and the Act amending the Police Act and certain other acts of January 2016. The Committee is particularly concerned about: a) the unlimited and indiscriminate surveillance of communications and collection of metadata b) the targeting of foreign nationals and application of different legal criteria to them, c) the insufficient procedural safeguards, d) the lack of adequate judicial oversight e) the possibility of banning or terminating assemblies and mass events; and f) the lack of notification, complaints procedure or mechanism for remedies.

40. The State party should review its counterterrorism legislation in order to bring it into line with its obligations under the Covenant, and ensure that any interference with the right to privacy complies with the principles of legality, necessity and proportionality."

Concluding Observations on the Second Periodic Report of Turkmenistan, Human Rights Committee, U.N. Doc. CCPR/C/TKM/CO/2 (28 March 2017)

"36. The Committee is concerned about the lack of a clear legal framework regulating surveillance activities including by the intelligence services (art. 17).

37. The State party should ensure that: (a) all types of surveillance activities and interference with privacy, including online surveillance for the purposes of State security, are governed by appropriate legislation that is in full conformity with the Covenant, in particular article 17, including with the principles of legality, proportionality and necessity, and that State practice conforms thereto; (b) surveillance is subject to judicial authorization as well as effective and independent oversight mechanisms; and (c) affected persons have proper access to effective remedies in cases of abuse."

Concluding Observations on the Second Periodic Report of Honduras, Human Rights Committee, U.N. Doc. CCPR/C/HND/CO/2 (27 July 2017) (translated from the original Spanish)

"38. The Committee is concerned about allegations regarding the frequent application of the Special Law on the Interception of Private Communications, which entails extensive monitoring of private communications. It also concerned about the lack of sufficient information regarding the grounds and evidence needed to obtain judicial authorization for surveillance operations...

39. The State party should take all necessary measures to ensure that its monitoring activities are in line with its obligations under the Covenant, especially Article 17, and that any interference with the right to privacy is in accordance with the principles Of legality, necessity and proportionality..."

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"23. ...any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear, and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances...

28. The State must ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that (a) are publicly accessible; (b) contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims; (c) are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected; and (d) provide for effective safeguards against abuse."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"35. Article 17 of the Covenant explicitly provides that everyone has the right to the protection of the law against unlawful or arbitrary interference with their privacy. This imports a "quality of law" requirement that imposes three conditions: (a) the measure must have some basis in domestic law; (b) the domestic law itself must be compatible with the rule of law and the requirements of the Covenant; and (c) the relevant provisions of domestic law must be accessible, clear and precise."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/HRC/34/61 (21 February 2017)

"36. The fact that surveillance powers are contained in public legislation is crucial to satisfying the principle of legality. The Special Rapporteur welcomes efforts by States to place intrusive surveillance regimes on a statutory footing, so that they can be subjected to public and parliamentary debate. However, publicly available primary legislation is not, in itself, sufficient to ensure the compatibility of those regimes with international human rights law. Necessity, proportionality and non-discrimination must also be taken into account along with the establishments of safeguards against arbitrariness, independent oversight and routes for redress."

Malone v. The United Kingdom, App. No. 8691/79, European Court of Human Rights, Judgment, Concurring Opinion of Judge Pettiti (2 August 1984)

"The danger threatening democratic societies in the years 1980-1990 stems from the temptation facing public authorities to "see into" the life of the citizen. In order to answer the needs of planning and of social and tax policy, the State is obliged to amplify the scale of its interferences. In its administrative systems, the State is being led to proliferate and then to computerise its personal data-files. Already in several of the member States of the Council of Europe each citizen is entered on 200 to 400 data-files. At a further stage, public authorities seek, for the purposes of their statistics and decision-making processes, to build up a "profile" of each citizen. Enquiries become more numerous; telephone tapping constitutes one of the favoured means of this permanent investigation.

Telephone tapping has during the last thirty years benefited from many "improvements" which have aggravated the dangers of interference in private life. The product of the interception can be stored on magnetic tapes and processed in postal or other centres equipped with the most sophisticated material. The amateurish tapping effected by police officers or post office employees now exists only as a memory of pre-war novels. The encoding of programmes and tapes, their decoding, and computer processing make it possible for interceptions to be multiplied a hundredfold and to be analysed in shorter and shorter time-spans, if need be by computer. Through use of the "mosaic" technique, a complete picture can be assembled of the life-style of even the "model" citizen. It would be rash to believe that the number of telephone interceptions is only a few hundred per year in each country and that they are all known to the authorities. Concurrently with developments in the techniques of interception, the aims pursued by the authorities have diversified. Police interception for the prevention of crime is only one of the practices employed; to this should be added political interceptions, interceptions of communications of journalists and leading figures, not to mention interceptions required by national defence and State security, which are included in the "top-secret" category and not dealt with in the Court's judgment or the present opinion...

The interference caused by interception of communications is more serious than an ordinary interference since the "innocent" victim is incapable of discovering it. If, as the British Government submitted, only the suspected criminal is placed under secret surveillance, there can be no ground for denying a measure involving judicial or equivalent control, or for refusing to have a neutral and impartial body situated between the authority deciding on the interception and the authority responsible for controlling the legality of the operation and its conformity with the legitimate aims pursued. The requirement of judicial control over telephone interceptions does not flow solely from a concern rooted in a philosophy of power and institutions but also from the necessities of protecting private life. In reality, even justified and properly controlled telephone interceptions call for counter-measures such as the right of access by the subject of the interception when the judicial phase has terminated in the discharge or acquittal of the accused, the right to erasure of the data obtained, the right of restitution of the tapes."

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

"84. The Court reiterates that the expression "in accordance with the law" within the meaning of Article 8 § 2 requires, firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law…"

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, European Court of Human Rights, Judgment (28 June 2007)

"71. The expression "in accordance with the law", as used in Article 8 § 2, does not only require that the impugned measure should have some basis in domestic law. It also refers to the quality of this law, demanding that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him or her, and compatible with the rule of law."

Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)

"38. Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

Escher et al. v. Brazil, Inter-American Court of Human Rights, Judgment (on Preliminary Objections, Merits, Reparations, and Costs), Series C No. 200 (6 July 2009)

"129. Since the telephone conversations of the alleged victims were private and they had not authorized that their conversations be conveyed to third parties, the interception of the conversations by State agents constituted interference in their private life. Therefore, the Court must examine whether this interference was arbitrary or abusive in the terms of Article 11(2) of the Convention or whether it was compatible with the said treaty. As indicated previously (supra para. 116), to conform to the American Convention any interference must comply with the following requirements: (a) it must be established by law; (b) it must have a legitimate purpose, and (c) it must be appropriate, necessary and proportionate. Consequently, the absence of any of these requirements implies that the interference is contrary to the Convention...

131. Taking into account that telephone interception can represent a serious interference in the private life of an individual, this measure must be based on a law that must be precise and indicate the corresponding clear and detailed rules, such as the circumstances in which this measure can be adopted, the persons authorized to request it, to order it and to carry it out, and the procedure to be followed."

Ms. X and Y v. Argentina, Inter-American Commission on Human Rights, Case 10.506, Report No. 38/96 (15 October 1996)

"91. ...The object of Article 11, as well as of the entire Convention, is essentially to protect the individual against arbitrary interference by public officials. Nevertheless, it also requires the state to adopt all necessary legislation in order to ensure this provision's effectiveness. The right to privacy guarantees that each individual has a sphere into which no one can intrude, a zone of activity which is wholly one's own. In this sense, various guarantees throughout the Convention which protect the sanctity of the person create zones of privacy.

92. Article 11.2 specifically prohibits "arbitrary or abusive" interference with this right. This provision indicates that in addition to the condition of legality, which should always be observed when a restriction is imposed on the rights of the Convention, the state has a special

obligation to prevent "arbitrary or abusive" interferences. The notion of "arbitrary interference" refers to elements of injustice, unpredictability and unreasonableness which were already considered by this Commission when it addressed the issues of the necessity, reasonableness, and proportionality of the searches and inspections."

i. Accessibility Requirement (extended)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"36. Accessibility requires not only that domestic law be published, but also that it meet a standard of clarity and precision sufficient to enable those affected to regulate their conduct with foresight of the circumstances in which intrusive surveillance may occur... Prior to the introduction of mass surveillance programmes outlined in the present report, [it had always been understood that it was required for] domestic legislation to spell out clearly the conditions under which, and the procedures by which, any interference may be authorized; the categories of person whose communications may be intercepted; the limits on the duration of surveillance; and the procedures for the use and storage of the data collected...

60. ...there is an urgent need for States using [Mass Surveillance] technology to revise and update national legislation to ensure consistency with international human rights law. Not only is this a requirement of Article 17, but it also provides an important opportunity for informed debate that can raised public awareness and enable individuals to make informed choices. Where the privacy rights of the entire digital community are at stake, nothing short of detailed and explicit primary legislation should suffice."

John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, Brief of Amici Curiae, United Nations Human Rights Experts in Support of Plaintiff-Appellant and Reversal, D.C. Ct. App., Case No. 16-7081, pp. 13-14, 16-17 (1 November 2016)

"Once an Individual has established a restriction on freedom of expression, the burden falls on the State Party to the Covenant to demonstrate that the restriction complies with the requirements of Article 19(3). Ethiopia likely cannot satisfy this burden. Its surveillance activities on Kidane's computer were conducted without evident legal justification, and therefore were not "provided by law". The condition of legality requires at least some public showing that the activity was authorized under formally enacted domestic laws and regulations. And even if Ethiopia provides justifications *ex post facto*, the law(s) it relies on must be "formulated with sufficient precision" and "may not confer unfettered discretion for the restriction freedom of expression on those charged with its execution" – a standard it is unlikely to meet given the indiscriminate nature of its alleged intrusion into Kidane's private communications...

Ethiopia's alleged surveillance activities interfere with Kidane's general right to privacy, which, by its very definition, protects "an area of anonymous development interaction, and liberty … free from State intervention." The interception and collection of Kidane's Skype phone calls, e-mails and other communications also interfered with the privacy of his correspondence. Correspondence "primarily means written letters, [but] today covers all forms of communications over distance, i.e., by telephone, telegram, telex, telefax, e-mail and other mechanical or electronic means of communications." The privacy of such correspondence

requires that it "should be delivered to the addressee without interception and without being opened or otherwise read."

Ethiopia's surveillance activities are "arbitrary and unlawful" under Article 17(1). The term "unlawful" implies that no interference can take place "except in cases envisaged by the law." Ethiopia's lack of evident legal justification for its surveillance of Kidane is "unlawful" for the same reasons it fails to satisfy the "provided by law" requirement under Article 19(3)."

Liberty and Others v. The United Kingdom, App. No. 58243/00, European Court of Human Rights, Judgment (1 July 2008)

"66. Under section 6 of the 1985 Act, the Secretary of State, when issuing a warrant for the interception of external communications, was called upon to "make such arrangements as he consider[ed] necessary" to ensure that material not covered by the certificate was not examined and that material that was certified as requiring examination was disclosed and reproduced only to the extent necessary. The applicants contend that material was selected for examination by an electronic search engine, and that search terms, falling within the broad categories covered by the certificates, were selected and operated by officials. According to the Government, there were at the relevant time internal regulations, manuals and instructions applying to the processes of selection for examination, dissemination and storage of intercepted material, which provided a safeguard against abuse of power. The Court observes, however, that details of these "arrangements" made under section 6 were not contained in legislation or otherwise made available to the public.

67. The fact that the Commissioner in his annual reports concluded that the Secretary of State's "arrangements" had been complied with, while an important safeguard against abuse of power, did not contribute towards the accessibility and clarity of the scheme, since he was not able to reveal what the "arrangements" were. In this connection the Court recalls its above case-law to the effect that the procedures to be followed for examining, using and storing intercepted material, inter alia, should be set out in a form which is open to public scrutiny and knowledge.

68. The Court notes the Government's concern that the publication of information regarding the arrangements made by the Secretary of State for the examination, use, storage, communication and destruction of intercepted material during the period in question might have damaged the efficacy of the intelligence-gathering system or given rise to a security risk. However, it observes that the German authorities considered it safe to include in the G10 Act, as examined in Weber and Saravia, express provisions about the treatment of material derived from strategic interception as applied to non-German telephone connections. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order. Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail in section 3(6) and (7) and section 7(4) of the amended G10 Act. The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of

external communications. In the United Kingdom, extensive extracts from the Code of Practice issued under section 71 of the 2000 Act are now in the public domain, which suggests that it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.

69. In conclusion, the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law"."

Kennedy v. The United Kingdom, App. No. 26839/05, European Court of Human Rights, Judgment (18 May 2010)

"157. In the present case, the Court notes, first, that the Code is a public document and is available on the Internet. Prior to its entry into force, it was laid before Parliament and approved by both Houses. Those exercising duties relating to interception of communications must have regard to its provisions and the provisions of the Code may be taken into account by courts and tribunals. In light of these considerations, the Court finds that the provisions of the Code can be taken into account in assessing the foreseeability of the RIPA regime..."

Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015)

"239. It is common ground between the parties that almost all legal provisions governing secret surveillance... have been officially published and are accessible to the public. The parties disputed, however, whether the addendums to Order no. 70 by the Ministry of Communications met the requirements of accessibility.

240. The Court observes that the addendums to Order no. 70 have never been published in a generally accessible official publication, as they were considered to be technical in nature.

241. The Court accepts that the addendums to Order no. 70 mainly describe the technical requirements for the interception equipment to be installed by communications service providers. At the same time, by requiring that the equipment at issue must ensure that the law-enforcement authorities have direct access to all mobile telephone communications of all users and must not log or record information about interceptions initiated by the law-enforcement authorities, the addendums to Order No. 70 are capable of affecting the users' right to respect for their private life and correspondence. The Court therefore considers that they must be accessible to the public.

242. The publication of the Order in the Ministry of Communications' official magazine SvyazInform, distributed through subscription, made it available only to communications specialists rather than to the public at large. At the same time, the Court notes that the text of the Order, with the addendums, can be accessed through a privately-maintained internet legal database, which reproduced it from the publication in SvyazInform. The Court finds the lack of a generally accessible official publication of Order no. 70 regrettable. However, taking into

account the fact that it has been published in an official ministerial magazine, combined with the fact that it can be accessed by the general public through an internet legal database, the Court does not find it necessary to pursue further the issue of the accessibility of domestic law."

ii. Foreseeability Requirement (extended)

Concluding Observations on the Fifth Periodic Report of Sri Lanka, Human Rights Committee, U.N. Doc. CCPR/C/LKA/CO/5 (21 November 2014)

"The State Party should... adopt national legislation that clearly and narrowly defines the exceptional conditions under which former combatants could be subject to monitoring and surveillance."

Concluding Observations on the Second Periodic Report of Namibia, Human Rights Committee, U.N. Doc. CCPR/C/NAM/CO/2 (22 April 2016)

"37. The Committee notes with concern that interception centres seem operational despite the fact that their legal basis, part 6 of the Communications Act, is not yet in force. While noting the indication by the delegation that all interceptions must be authorized by a magistrate, and that no private information is kept, the Committee is concerned about the lack of clarity regarding the reach of legal interception possibilities, as well as about the safeguards to ensure respect of the right to privacy in line with the Covenant.

38. The State party should ensure that the interception of telecommunication s may only be justified under limited circumstances authorized by law with the necessary procedural and judicial safeguards against abuse, and supervised by the courts when in full conformity with the Covenant."

Concluding Observations on the Sixth Periodic Report of New Zealand, Human Rights Committee, U.N. Doc. CCPR/C/NZL/CO/6 (28 April 2016)

"15. The Committee is concerned that the right to privacy is not part of the Bill of Rights Act 1990 and that the existing legal framework provides the Government Communications Security Bureau with a very broad mandate. The Committee is also concerned about the absence of a clear definition of the terms "national security" and "private communication" in the Telecommunications (Interception Capability and Security) Act 2013...

16. The State Party should take all appropriate measures to ensure that: (a) Its legal framework regulating communications surveillance is in line with its obligations under the Covenant, in particular article 17;"

Concluding Observations on the Fourth Periodic Report of Rwanda, Human Rights Committee, U.N. Doc. CCPR/C/RWA/CO/4 (2 May 2016)

"35. The Committee is concerned that Law No. 60/2013 permits the interception of communications without prior authorization of a judge.

36. The State party should take legislative and other measures necessary to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity. It should also ensure that communications are intercepted and data are used to

achieve specific and legitimate objectives and that the categories of circumstances in which such interference may be authorized and the categories of persons whose communications are likely to be intercepted are set out in detail..."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (17 April 2013)

"83. Legal frameworks must ensure that communications surveillances measures: (a) are prescribed by law, meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application."

Leander v. Sweden, App. No. 9248/81, European Court of Human Rights, Judgment (26 March 1987)

"50. The expression "in accordance with the law" in paragraph 2 of Article 8 (art. 8-2) requires, to begin with, that the interference must have some basis in domestic law. Compliance with domestic law, however, does not suffice: the law in question must be accessible to the individual concerned and its consequences for him must also be foreseeable.

51. However, the requirement of foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally, as under the Personnel Control Ordinance, the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life. In assessing whether the criterion of foreseeability is satisfied, account may be taken also of instructions or administrative practices which do not have the status of substantive law, in so far as those concerned are made sufficiently aware of their contents. In addition, where the implementation of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

Kruslin v. France, App. No. 11801/85, European Court of Human Rights, Judgment (24 April 1990)

"28. ...The Delegate of the Commission considered that in the case of the Continental countries, including France, only a substantive enactment of general application - whether or not passed by Parliament - could amount to a "law" for the purposes of Article 8 § 2 (art. 8-2) of the Convention. Admittedly the Court had held that "the word 'law' in the expression 'prescribed by law' cover[ed] not only statute but also unwritten law", but in those instances the Court was, so the Delegate maintained, thinking only of the common-law system. That system, however, was radically different from, in particular, the French system. In the latter, case-law was undoubtedly a very important source of law, but a secondary one, whereas by "law" the Convention meant a primary source.

29. ...In relation to paragraph 2 of Article 8 (art. 8-2) of the Convention and other similar clauses, the Court has always understood the term "law" in its "substantive" sense, not its "formal" one; it has included both enactments of lower rank than and unwritten law. The *Sunday Times*, *Dudgeon*, and *Chappell* judgments admittedly concerned the United Kingdom, but it would be wrong to exaggerate the distinction between common-law countries and Continental countries, as the Government rightly pointed out... In a sphere covered by the written law, the "law" is the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments.

31. The Government submitted that the Court must be careful not to rule on whether French legislation conformed to the Convention in the abstract and not to give a decision based on legislative policy. The Court was therefore not concerned, they said, with matters irrelevant to Mr Kruslin's case, such as the possibility of telephone tapping in relation to minor offences or the fact that there was no requirement that an individual whose telephone had been monitored should be so informed after the event where proceedings had not in the end been taken against him. Such matters were in reality connected with the condition of "necessity in a democratic society", fulfilment of which had to be reviewed in concrete terms, in the light of the particular circumstances of each case.

32. The Court is not persuaded by this argument. Since it must ascertain whether the interference complained of was "in accordance with the law", it must inevitably assess the relevant French "law" in force at the time in relation to the requirements of the fundamental principle of the rule of law. Such a review necessarily entails some degree of abstraction. It is none the less concerned with the "quality" of the national legal rules applicable to Mr Kruslin in the instant case."

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, European Court of Human Rights, Judgment (28 June 2007)

"75. In the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence. In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."

Liberty and Others v. The United Kingdom, App. No. 58243/00, European Court of Human Rights, Judgment (1 July 2008)

"60. ...[The Government responded] that although the scope of the executive's discretion to carry out surveillance had to be indicated in legislation, "the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law".

61. The Court observes, first, that the above passage from Malone was itself a reference to Silver and Others. There the Court accepted that administrative Orders and Instructions, which set out the detail of the scheme for screening prisoners' letters but did not have the force of law, could be taken into account in assessing whether the criterion of foreseeability was satisfied in the application of the relevant primary and secondary legislation, but only to "the admittedly limited extent to which those concerned were made sufficiently aware of their

contents". It was only on this basis – that the content of the Orders and Instructions were made known to the prisoners – that the Court was able to reject the applicants' contention that the conditions and procedures governing interferences with correspondence, and in particular the directives set out in the Orders and Instructions, should be contained in the substantive law itself.

63. It is true that the above requirements were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses (the equivalent, within the United Kingdom, of the section 3(1) regime). However, the Weber and Saravia case was itself concerned with generalised "strategic monitoring", rather than the monitoring of individuals. The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other..."

S. and Marper v. The United Kingdokm, App. Nos. 30562/04 and 30566/04, European Court of Human Rights, Judgment (4 December 2008)

"96. The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed."

Iordachi and Others v. Moldova, App. No. 25198/02, European Court of Human Rights, Judgment (24 September 2009)

"44. Still, the nature of the offences which may give rise to the issue of an interception warrant is not, in the Court's opinion, sufficiently clearly defined in the impugned legislation. In particular, the Court notes that more than one half of the offences provided for in the Criminal Code fall within the category of offences eligible for interception warrants. Moreover, the Court is concerned by the fact that the impugned legislation does not appear to define sufficiently clearly the categories of persons liable to have their telephones tapped. It notes that Article 156 § 1 of the Criminal Code uses very general language when referring to such persons and states that the measure of interception may be used in respect of a suspect, defendant or other person involved in a criminal offence. No explanation has been given as to who exactly falls within the category of "other person involved in a criminal offence".

45. The Court further notes that the legislation in question does not provide for a clear limitation in time of a measure authorising interception of telephone communications. While the Criminal Code imposes a limitation of six months, there are no provisions under the impugned legislation which would prevent the prosecution authorities from seeking and obtaining a new interception warrant after the expiry of the statutory six months' period.

46. Moreover, it is unclear under the impugned legislation who – and under what circumstances – risks having the measure applied to him or her in the interests of, for instance, protection of health or morals or in the interests of others. While enumerating in section 6 and in Article 156 § 1 the circumstances in which tapping is susceptible of being applied, the Law on Operational Investigative Activities and the Code of Criminal Procedure fails, nevertheless, to define "national security", "public order", "protection of health", "protection of morals", "protection of the rights and interests of others", "interests of ... the economic situation of the country" or

"maintenance of legal order" for the purposes of interception of telephone communications. Nor does the legislation specify the circumstances in which an individual may be at risk of having his telephone communications intercepted on any of those grounds."

Kennedy v. The United Kingdom, App. No. 26839/05, European Court of Human Rights, Judgment (18 May 2010)

"159. As to the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to interception. However, sufficient detail should be provided of the nature of the offences in question. In the case of RIPA, section 5 provides that interception can only take place where the Secretary of State believes that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or for the purposes of safeguarding the economic well-being of the United Kingdom. The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees. It observes that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which Article 8 § 2 itself refers. The Court has previously emphasised that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to deport an individual on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. Similar considerations apply to the use of the term in the context of secret surveillance. Further, additional clarification of how the term is to be applied in practice in the United Kingdom has been provided by the Commissioner, who has indicated that it allows surveillance of activities which threaten the safety or well-being of the State and activities which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means. As for "serious crime", this is defined in the interpretative provisions of the Act itself and what is meant by "detecting" serious crime is also explained in the Act. The Court is of the view that the reference to serious crime, together with the interpretative clarifications in the Act, gives citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures. The Court therefore considers that, having regard to the provisions of RIPA, the nature of the offences which may give rise to an interception order is sufficiently clear."

Uzun v. Germany, App. No. 35623/05, European Court of Human Rights, Judgment (2 September 2010)

"61. As to the requirement of legal "foreseeability" in this field, the Court reiterates that in the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any such measures...

62. The Court has further stated, in the context of Article 7 of the Convention, that in any system of law, including criminal law, however clearly drafted a legal provision may be, there is an inevitable element of judicial interpretation. There will always be a need for elucidation of doubtful points and for adaptation to changing circumstances. Indeed, in the Convention States, the progressive development of the criminal law through judicial law-making is a well entrenched and necessary part of legal tradition. The Convention cannot be read as outlawing the gradual clarification of the rules of criminal liability through judicial interpretation from case to case, provided that the resultant development is consistent with the essence of the

offence and could reasonably be foreseen. The Court considers that these principles, developed under Article 7, apply also in the present context..."

Shimovolos v. Russia, App. No. 30194/09, European Court of Human Rights, Judgment (21 June 2011)

"68. The Court reiterates in this connection that in the special context of secret measures of surveillance the above requirements cannot mean that an individual should be able to foresee when the authorities are likely to resort to secret surveillance so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on the application of secret measures of surveillance, especially as the technology available for use is continually becoming more sophisticated. The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to any measures of secret surveillance and collection of data. In addition, because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.

69. Turning to the present case, the Court observes that the creation and maintenance of the Surveillance Database and the procedure for its operation are governed by ministerial order no. 47. That order is not published and is not accessible to the public. The grounds for registration of a person's name in the database, the authorities competent to order such registration, the duration of the measure, the precise nature of the data collected, the procedures for storing and using the collected data and the existing controls and guarantees against abuse are thus not open to public scrutiny and knowledge.

70. For the above reasons, the Court does not consider that the domestic law indicates with sufficient clarity the scope and manner of exercise of the discretion conferred on the domestic authorities to collect and store in the Surveillance Database information on persons' private lives. In particular, it does not, as required by the Court's case-law, set out in a form accessible to the public any indication of the minimum safeguards against abuse. The interference with the applicant's rights under Article 8 was not, therefore, "in accordance with the law".

Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015)

"243. The Court reiterates that the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures – in particular by clearly setting out the nature of the offences which may give rise to an interception order and a definition of the categories of people liable to have their telephones tapped.

244. As regards the nature of the offences, the Court emphasises that the condition of foreseeability does not require States to set out exhaustively, by name, the specific offences which may give rise to interception. However, sufficient detail should be provided on the nature of the offences in question. Both the OSAA and the CCrP provide that telephone and other communications may be intercepted in connection with an offence of medium severity, a

serious offence or an especially serious criminal offence – that is, an offence for which the Criminal Code prescribes a maximum penalty of more than three years' imprisonment – which has been already committed, is ongoing or being plotted. The Court considers that the nature of the offences which may give rise to an interception order is sufficiently clear. At the same time it notes with concern that Russian law allows secret interception of communications in respect of a very wide range of criminal offences, including for example, as pointed out by the applicant, pickpocketing.

245. The Court further notes that interceptions may be ordered not only in respect of a suspect or an accused, but also in respect of a person who may have information about an offence or may have other information relevant to the criminal case. The Court has earlier found that interception measures in respect of a person who was not suspected of any offence but could possess information about such an offence might be justified under Article 8 of the Convention. At the same time, the Court notes the absence of any clarifications in Russian legislation or established case-law as to how the terms "a person who may have information about a criminal offence" and "a person who may have information relevant to the criminal case" are to be applied in practice.

246. The Court also observes that in addition to interceptions for the purposes of preventing or detecting criminal offences, the OSAA also provides that telephone or other communications may be intercepted. following the receipt of information about events or activities endangering Russia's national, military, economic or ecological security. Which events or activities may be considered as endangering such types of security interests is nowhere defined in Russian law.

247. The Court has previously found that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to subject an individual to secret surveillance on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance. At the same time, the Court has also emphasised that in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

248. It is significant that the OSAA does not give any indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering Russia's national, military, economic or ecological security. It leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse."

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

"64. ...the wording of many statutes is not absolutely precise, and that the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague. It is satisfied that

even in the field of secret surveillance, where foreseeability is of particular concern, the danger of terrorist acts and the needs of rescue operations are both notions sufficiently clear so as to meet the requirements of lawfulness. For the Court, the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all situations that may prompt a decision to launch secret surveillance operations. The reference to terrorist threats or rescue operations can be seen in principle as giving citizens the requisite indication. For the Court, nothing indicates in the text of the relevant legislation that the notion of "terrorist acts", as used in section 7/E (1) a) (ad) of the Police Act, does not correspond to the crime of the same denomination contained in the Criminal Code.

65. However, in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.

66. The Court notes that under "section 7/E (3) surveillance", it is possible for virtually any person in Hungary to be subjected to secret surveillance. The legislation does not describe the categories of persons who, in practice, may have their communications intercepted. In this respect, the Court observes that there is an overlap between the condition that the categories of persons be set out and the condition that the nature of the underlying situations be clearly defined. The relevant circumstances which can give rise to interception, discussed in the preceding paragraphs, give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted. Under the relevant Hungarian law, the proposal submitted to the responsible government minister must specify, either by name or as a range of persons, the person or persons as the interception subjects and/or any other relevant information capable of identifying them as well as the premises in respect of which the permission is sought.

67. It is of serious concern, however, that the notion of "persons concerned identified ... as a range of persons" might include indeed any person and be interpreted as paving the way for the unlimited surveillance of a large number of citizens. The Court notes the absence of any clarification in domestic legislation as to how this notion is to be applied in practice. For the Court, the category is overly broad, because there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons "concerned" and the prevention of any terrorist threat – let alone in a manner enabling an analysis by the authoriser which would go to the question of strict necessity with regard to the aims pursued and the means employed – although such an analysis appears to be warranted by section 53 (2) of the National Security Act, according to which "secret intelligence gathering [may only be applied] if the intelligence needed ... cannot be obtained in any other way"."

Escher et al. v. Brazil, Inter-American Court of Human Rights, Judgment (on Preliminary Objections, Merits, Reparations, and Costs), Series C No. 200 (6 July 2009)

"118. The Commission alleged that although the laws that authorize the interception and monitoring of telephone or any other type of communications were formulated to combat crime, they can become an instrument for spying and harassment if they are interpreted and applied improperly. Hence, owing to the inherent danger of abuse in any monitoring system,

this measure must be based on especially precise legislation with clear, detailed rules. The American Convention protects the confidentiality and inviolability of communications from any kind of arbitrary or abusive interference from the State or individuals; consequently, the surveillance, intervention, recording and dissemination of such communications is prohibited, except in the cases established by law that are adapted to the objects and purposes of the American Convention."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"155. ...the existence of a law is not enough for a program to be legitimate. As previously mentioned, vague or ambiguous legal provisions that grant very broad discretionary powers are incompatible with the American Convention, because they can serve as the basis for potential arbitrary acts that translate into violations of the right to privacy or the right to freedom of thought and expression guaranteed by the Convention.

156. The laws that authorize the interception of communications must establish clearly and precisely the reasons the State can invoke to request that interception, which can only be authorized by a judge. Additionally, must be established by law safeguards pertaining to the nature, scope, and duration of the surveillance measures; the facts that could justify these measures, and the authorities competent to authorize them, carry them out, and supervise them. The law must be clear with regard to the possible remedies for abuses committed in the exercise of those powers.

157. Second, limitations to the rights guaranteed by the American Convention must pursue compelling objectives agreed to by the States through their signature of international human rights law instruments. In the case of State surveillance activities—on the Internet or in any other sphere—reasons of national security and the fight against crime or organized crime tend to be invoked. The Office of the Special Rapporteur has maintained that when national security is invoked as a reason for monitoring personal data and correspondence, in order to prevent discretionary interpretations, the law must clearly specify the criteria to be applied in determining the cases in which these types of limitations are legitimate, and it must be careful to define that concept precisely. In particular, the Office of the Special Rapporteur has asserted that the concept of national security cannot be interpreted haphazardly and must be defined from a democratic perspective.

158. The inter-American system for the protection of human rights has ruled, for example, on inadmissible interpretations of the concept of national security. In the case of *Molina-Theissen v. Guatemala*, the Inter-American Court of Human Rights held that the so-called "national security doctrine" makes it possible to characterize a person as 'subversive' or as an 'internal enemy,' for the sole fact that they genuinely or allegedly supported the fight to change the established order. Similarly, in the case of *Goiburu et al. v. Paraguay* the Court found that "[m]ost of the Southern Cone's dictatorial governments assumed power or were in power during the 1970s [...]. The ideological basis of all these regimes was the 'National Security Doctrine,' which regarded leftist movements and other groups as 'common enemies'." Even today, it has been reported that national security reasons tend to be invoked to place human rights defenders, journalists, members of the media, and activists under surveillance, or to justify excessive secrecy in the decision-making processes and investigations tied to surveillance issues. Clearly, this kind of interpretation of the "national security" objective

cannot be the basis for the establishment of surveillance programs of any kind, including, naturally, online communications surveillance programs."

B. The Principle of Necessity (extended)

U.N. Human Rights Committee, *Toonen v. Australia*, Comm. No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (31 March 1994)

"8.3 ...any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (17 April 2013)

"83. Legal frameworks must ensure that communications surveillances measures: ... (b) are strictly and demonstrably necessary to achieve a legitimate aim."

Klass and Others v. Germany, App. No. 5029/71, European Court of Human Rights, Judgment (6 September 1978)

"42. The cardinal issue arising under Article 8 (art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions...

47. The applicants do not object to the German legislation in that it provides for wide-ranging powers of surveillance; they accept such powers, and the resultant encroachment upon the right guaranteed by Article 8 para. 1 (art. 8-1), as being a necessary means of defence for the protection of the democratic State. The applicants consider, however, that paragraph 2 of Article 8 (art. 8-2) lays down for such powers certain limits which have to be respected in a democratic society in order to ensure that the society does not slide imperceptibly towards totalitarianism. In their view, the contested legislation lacks adequate safeguards against possible abuse.

48. As the Delegates observed, the Court, in its appreciation of the scope of the protection offered by Article 8 (art. 8), cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.

49. As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field. Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."

Malone v. The United Kingdom, App. No. 8691/79, European Court of Human Rights, Judgment (2 August 1984)

"81. Undoubtedly, the existence of some law granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be "necessary in a democratic society ... for the prevention of disorder or crime", within the meaning of paragraph 2 of Article 8 (art. 8-2). The Court accepts, for example, the assertion in the Government's White Paper (at para. 21) that in Great Britain "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have made telephone interception an indispensable tool in the investigation and prevention of serious crime". However, the exercise of such powers, because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole. This being so, the resultant interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse."

Leander v. Sweden, App. No. 9248/81, European Court of Human Rights, Judgment (26 March 1987)

"58. The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.

59. However, the Court recognises that the national authorities enjoy a margin of appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life. There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power, firstly, to collect and store in registers not accessible to the public information on persons and, secondly, to use this information when assessing the suitability of candidates for employment in posts of importance for national security."

Rotaru v. Romania, App. No. 28341/95, European Court of Human Rights, Judgment (4 May 2000)

"47. The cardinal issue that arises is whether the interference so found is justifiable under paragraph 2 of Article 8. That paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be interpreted narrowly. While the Court recognises that intelligence

services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."

Dragojević v. Croatia, App. No. 68955/11, European Court of Human Rights, Judgment (15 January 2015)

"83. ...in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist guarantees against abuse which are adequate and effective. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.

84. This in particular bears significance as to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, since the Court has held that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In assessing the existence and extent of such necessity the Contracting States enjoy a certain margin of appreciation but this margin is subject to European supervision. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded...

89. ...the central question for the Court to determine is whether the relevant domestic law, including the way in which it was interpreted by the domestic courts, indicated with reasonable clarity the scope and manner of exercise of the discretion conferred on the public authorities, and in particular whether the domestic system of secret surveillance, as applied by the domestic authorities, afforded adequate safeguards against various possible abuses. Since the existence of adequate safeguards against abuse is a matter closely related to the question whether the "necessity" test was complied with in this case, the Court will address both the requirement that the interference be "in accordance with the law" and that it be "necessary"...

97. It follows from the foregoing that whereas the Code of Criminal Procedure expressly envisaged prior judicial scrutiny and detailed reasons when authorising secret surveillance orders, in order for such measures to be put in place, the national courts introduced the possibility of retrospective justification of their use, even where the statutory requirement of prior judicial scrutiny and detailed reasons in the authorisation was not complied with. In an area as sensitive as the use of secret surveillance, which is tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions, the Court has difficulty in accepting this situation created by the national courts...

98. Moreover, the Court considers that in a situation where the legislature envisaged prior detailed judicial scrutiny of the proportionality of the use of secret surveillance measures, a circumvention of this requirement by retrospective justification, introduced by the courts, can hardly provide adequate and sufficient safeguards against potential abuse since it opens the

door to arbitrariness by allowing the implementation of secret surveillance contrary to the procedure envisaged by the relevant law."

Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015)

"232. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society"...

236. In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements. The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse.

237. It has not been disputed by the parties that interceptions of mobile telephone communications have a basis in the domestic law. They are governed, in particular, by the CCrP and the OSAA, as well as by the Communications Act and the Orders issued by the Ministry of Communications. Furthermore, the Court considers it clear that the surveillance measures permitted by Russian law pursue the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country. It therefore remains to be ascertained whether the domestic law is accessible and contains adequate and effective safeguards and guarantees to meet the requirements of "foreseeability" and "necessity in a democratic society".

238. The Court will therefore assess in turn the accessibility of the domestic law, the scope and duration of the secret surveillance measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, the authorisation procedures, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law."

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment, Concurring Opinion of Judge Pinto De Albuquerque (12 January 2016)

"21. [The] judgment use[s] a "strict necessity" test and refer it to two purposes: the safeguarding of democratic institutions and the acquiring of vital intelligence in an individual operation. his creative rephrasing of the legal test raises several problems. Firstly, it is a stricter criterion than that in paragraphs 233 and 236 of Roman Zakharov. Secondly, it does not match the looser criterion for the degree of suspicion of involvement in the offences or activities being monitored. It is logically inconsistent that the same judgment imposes a "strict necessity" test for the determination of the surveillance measure, but at the same time accepts a very loose criterion for the degree of suspicion of involvement in the offences or activities being monitored, as demonstrated above. It is logically incoherent to criticise the overly broad text of the Hungarian law when it refers to the "persons concerned identified as a range of persons" and yet to accept the linguistically vague and legally imprecise "individual suspicion" test to ground the applicability of a surveillance measure. Thirdly, the Chamber did not clarify in what the "strict necessity test" consists, having merely linked the test to the purposes pursued. Nowhere does the judgment clarify that the necessity test warrants that any surveillance operation be ordered only if the establishment of the facts by other less intrusive methods has proven unsuccessful or, exceptionally, if other less intrusive methods are deemed unlikely to succeed."

Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)

"42. It is apparent from the case-law of the Court that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest. The same is true of the fight against serious crime in order to ensure public security. Furthermore, it should be noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security.

43. In this respect, it is apparent from recital 7 in the preamble to Directive 2006/24 that, because of the significant growth in the possibilities afforded by electronic communications, the Justice and Home Affairs Council of 19 December 2002 concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.

44. It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive 2006/24, genuinely satisfies an objective of general interest...

51. As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.

52. So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"159. ...in order for an online communications surveillance program to be appropriate, States must demonstrate that the limitations to the rights to privacy and freedom of expression arising from those programs are strictly necessary in a democratic society to accomplish the objectives they pursue.

160. The opinion of strict necessity with respect to communications surveillance assumes that it is insufficient for the measure to be "useful," "reasonable," or "opportune." In order for the restriction to be legitimate, the true and compelling need to impose the limitation must be clearly established; that is, said legitimate and compelling aim cannot be reasonably accomplished by any other means less restrictive of human rights."

C. The Principle of Proportionality (extended)

U.N. Human Rights, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (8 April 1988)

"The expression "arbitrary interference" is also relevant to the protection of the right provided for in article 17. In the Committee's view the expression "arbitrary interference" 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."

U.N. Human Rights Committee, *Toonen v. Australia*, Comm. No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (31 March 1994)

"8.3 ...any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/HRC/13/37 (28 December 2009)

"49. [Right to Privacy protections] require States to have exhausted less-intrusive techniques before resorting to others... States must incorporate this principle into existing and future policies as they present how their policies are necessary, and in turn proportionate"

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (17 April 2013)

"83. Legal frameworks must ensure that communications surveillances measures: ... (c) adhere to the principle of proportionality, and are not employed when less invasive techniques are available or have not yet been exhausted."

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"23. These authoritative sources [HRC General Comments 16, 27, 29, 31, and 34 and the Siracusa Principles] point to the overarching principles of legality, necessity and proportionality... The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary."

U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017)

"...Recognizing the need to further discuss and analyse, on the basis of international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness, lawfulness, legality, necessity and proportionality in relation to surveillance practices...

2. Recalls that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality"

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"161. In any case, as has been mentioned, in order to define if a measure is proportioned, its impact on the capacity of the Internet to guarantee and promote freedom of expression should be evaluated.

162. Given the importance of the exercise of these rights in a democratic system, the law must authorize access to personal data and communications only under the most exceptional circumstances defined in the law. When fairly open-ended grounds such as national security are invoked as the reason to monitor personal data and correspondence, the law must clearly specify the criteria to be applied in determining those cases in which such limitations are legitimate. Their application should be authorized solely when there is a definite risk to the protected interests, and when that harm is greater than society's general interest in maintaining the rights to privacy and the free expression of thought and the circulation of information."

Draft agreement between Canada and the European Union on the Transfer of Passenger Name Record data (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)

"140. As regards observance of the principle of proportionality, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary...

141. In order to satisfy that requirement, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing. Those considerations apply particularly where the protection of the particular category of personal data that is sensitive data is at stake…

156. ...heading 5, which refers to 'available frequent flyer and benefit information (free tickets, upgrades, etc.)', and heading 7, which covers 'all available contact information (including originator information)', do not define in a sufficiently clear and precise manner the PNR data to be transferred.

157. Thus, as regards heading 5, the use of the term 'etc.' does not specify to the requisite standard the scope of the data to be transferred. Furthermore, it is not clear from the terms of that heading whether it covers information concerning merely the status of air passengers in customer loyalty programmes or whether, on the contrary, it covers all information relating to air travel and transactions carried out in the context of such programmes.

158. Similarly, the use of the terms 'all available contact information' in heading 7 does not specify sufficiently the scope of the data to be transferred. In particular, it does not specify what type of contact information is covered, nor does it specify whether that contact information also covers [...] the contact information of third parties who made the flight reservation for the air passenger, third parties through whom an air passenger may be contacted, or indeed third parties who are to be informed in the event of an emergency...

160. As regards heading 17, that heading refers to 'general remarks including Other Supplementary Information (OSI), Special Service Information (SSI) and Special Service Request (SSR) information'. According to the explanations provided, inter alia, by the Commission, that heading constitutes a 'free text' heading, intended to include 'all supplementary information', in addition to that listed elsewhere in the Annex to the envisaged agreement. Consequently, such a heading provides no indication as to the nature and scope of the information to be communicated, and it may even encompass information entirely unrelated to the purpose of the transfer of PNR data. Furthermore, since the information referred to in that heading is listed only by way of example, as is shown by the use of the term 'including', heading 17 does not set any limitation on the nature and scope of the information that could be set out thereunder. In those circumstances, heading 17 cannot be regarded as being delimited with sufficient clarity and precision."

D. The Principle of Adequate Safeguards (extended)

Klass and Others v. Germany, App. No. 5029/71, European Court of Human Rights, Judgment (6 September 1978)

"50. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law…

59. Both in general and in relation to the question of subsequent notification, the applicants have constantly invoked the danger of abuse as a ground for their contention that the legislation they challenge does not fulfil the requirements of Article 8 para. 2 (art. 8-2) of the Convention. While the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system, the considerations that matter for the purposes of the Court's present review are the likelihood of such action and the safeguards provided to protect against it. The Court has examined above the contested legislation in the light, inter alia, of these considerations. The Court notes in particular that the G 10 contains various provisions designed to reduce the effect of surveillance measures to an unavoidable minimum and to ensure that the surveillance is carried out in strict accordance with the law. In the absence of any evidence or indication that the actual practice followed is otherwise, the Court must assume that in the democratic society of the Federal Republic of Germany, the relevant authorities are properly applying the legislation in issue. The Court agrees with the Commission that some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention. As the Preamble to the Convention states, "Fundamental Freedoms ... are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which (the Contracting States) depend". In the context of Article 8 (art. 8), this means that a balance must be sought between the exercise by the individual of the right guaranteed to him under paragraph 1 (art. 8-1) and the necessity under paragraph 2 (art. 8-2) to impose secret surveillance for the protection of the democratic society as a whole."

Leander v. Sweden, App. No. 9248/81, European Court of Human Rights, Judgment (26 March 1987)

"60. ... in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse."

Kopp v. Switzerland, App. No. 23224/94, European Court of Human Rights, Judgment (25 March 1998)

"71. ...[The Government] added that Mr Kopp, the husband of a former member of the Federal Council, had not had his telephones tapped in his capacity as a lawyer. In the instant case, in accordance with Swiss telephone-monitoring practice, a specialist Post Office official had listened to the tape in order to identify any conversations relevant to the proceedings in

progress, but no recording had been put aside and sent to the Federal Public Prosecutor's Office.

72. The Court, however, is not persuaded by these arguments. Firstly, it is not for the Court to speculate as to the capacity in which Mr Kopp had had his telephones tapped, since he was a lawyer and all his law firm's telephone lines had been monitored. Secondly, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated. In that connection, the Court by no means seeks to minimise the value of some of the safeguards built into the law, such as the requirement at the relevant stage of the proceedings that the prosecuting authorities' telephone-tapping order must be approved by the President of the Indictment Division, who is an independent judge, or the fact that the applicant was officially informed that his telephone calls had been intercepted.

73. However, the Court discerns a contradiction between the clear text of legislation which protects legal professional privilege when a lawyer is being monitored as a third party and the practice followed in the present case. Even though the case-law has established the principle, which is moreover generally accepted, that legal professional privilege covers only the relationship between a lawyer and his clients, the law does not clearly state how, under what conditions and by whom the distinction is to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to activity other than that of counsel.

74. Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence.

75. In short, Swiss law, whether written or unwritten, does not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter. Consequently, Mr Kopp, as a lawyer, did not enjoy the minimum degree of protection required by the rule of law in a democratic society. There has therefore been a breach of Article 8."

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, European Court of Human Rights, Judgment (28 June 2007)

"92. ...the Court notes that the Bulgarian Supreme Cassation Prosecutor's Office apparently found, in a report of January 2001, that numerous abuses had taken place. According to this report, more than 10,000 warrants were issued over a period of some twenty-four months, from 1 January 1999 to 1 January 2001, and that number does not even include the tapping of mobile telephones (for a population of less than 8,000,000). Out of these, only 267 or 269 had subsequently been used in criminal proceedings. A significant number of breaches of the law had been observed. Additionally, in an interview published on 26 January 2001 the then Minster of Internal Affairs conceded that he had signed 4,000 orders for the deployment of means of secret surveillance during his thirteen months in office. By contrast, in Malone, the number of the warrants issued was considered relatively low (400 telephone tapping warrants and less than 100 postal warrants annually during the period 1969-79, for more than 26,428,000 telephone lines nationwide). These differences are telling, even if allowance is made for the

development of the means of communication and the rise in terrorist activities in recent years. They also show that the system of secret surveillance in Bulgaria is, to say the least, overused, which may in part be due to the inadequate safeguards which the law provides."

Kennedy v. The United Kingdom, App. No. 26839/05, European Court of Human Rights, Judgment (18 May 2010)

"160. The Court observes that under RIPA, it is possible for the communications of any person in the United Kingdom to be intercepted. However, it should be recalled that, in contrast to the Liberty and Others case which concerned the legislation on interception of communications between the United Kingdom and any other country, the present case concerns internal communications, i.e. communications within the United Kingdom. Further, the legislation must describe the categories of persons who, in practice, may have their communications intercepted. In this respect, the Court observes that there is an overlap between the condition that the categories of persons be set out and the condition that the nature of the offences be clearly defined. The relevant circumstances which can give rise to interception, discussed in the preceding paragraph, give guidance as to the categories of persons who are likely, in practice, to have their communications intercepted. Finally, the Court notes that in internal communications cases, the warrant itself must clearly specify, either by name or by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered. Names, addresses, telephone numbers and other relevant information must be specified in the schedule to the warrant. Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA. The Court considers that, in the circumstances, no further clarification in the legislation or the Code of the categories of persons liable to have their communications intercepted can reasonably be required.

161. In respect of the duration of any telephone tapping, the Act clearly stipulates, first, the period after which an interception warrant will expire and, second, the conditions under which a warrant can be renewed. Although a warrant can be renewed indefinitely, the Secretary of State himself must authorise any renewal and, upon such authorisation, must again satisfy himself that the warrant remains necessary on the grounds stipulated in section 5(3). In the context of national security and serious crime, the Court observes that the scale of the criminal activities involved is such that their planning often takes some time. Subsequent investigations may also be of some duration, in light of the general complexity of such cases and the numbers of individuals involved. The Court is therefore of the view that the overall duration of any interception measures will depend on the complexity and duration of the investigation in question and, provided that adequate safeguards exist, it is not unreasonable to leave this matter for the discretion of the relevant domestic authorities. The Code explains that the person seeking the renewal must make an application to the Secretary of State providing an update and assessing the value of the interception operation to date. He must specifically address why he considers that the warrant remains necessary on section 5(3) grounds. Further, under section 9(3) RIPA, the Secretary of State is obliged to cancel a warrant where he is satisfied that the warrant is no longer necessary on section 5(3) grounds. There is also provision in the Act for specific factors in the schedule to the warrant to be deleted where the Secretary of State considers that they are no longer relevant for identifying communications from or to the interception subject. The Code advises that the duty on the Secretary of State to cancel warrants which are no longer necessary means, in practice, that intercepting agencies must keep their warrants under continuous review. The Court concludes that the provisions on duration, renewal and cancellation are sufficiently clear."

Uzun v. Germany, App. No. 35623/05, European Court of Human Rights, Judgment (2 September 2010)

"63. ...in the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 rights. The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law...

65. As to the law's foreseeability and its compliance with the rule of law, the Court notes at the outset that in his submissions, the applicant strongly relied on the minimum safeguards which are to be set out in statute law in order to avoid abuses as developed by the Court in the context of applications concerning the interception of telecommunications. According to these principles, the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their communications monitored; a limit on the duration of such monitoring; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which data obtained may or must be erased or the records destroyed, have to be defined in statute law.

66. While the Court is not barred from gaining inspiration from these principles, it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications, are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations. It will therefore apply the more general principles on adequate protection against arbitrary interference with."

i. Reasonable Suspicion (extended)

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

"125. The Court finds that the transmission of personal data obtained by general surveillance measures without any specific prior suspicion in order to allow the institution of criminal proceedings against those being monitored constitutes a fairly serious interference with the right of these persons to secrecy of telecommunications."

S. and Marper v. The United Kingdokm, App. Nos. 30562/04 and 30566/04, European Court of Human Rights, Judgment (4 December 2008)

"122. Of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. In this respect, the Court must bear in mind that the right of every person

under the Convention to be presumed innocent includes the general rule that no suspicion regarding an accused's innocence may be voiced after his acquittal..."

Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015)

"260. Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means.

261. The Court notes that in Russia judicial scrutiny is limited in scope. Thus, materials containing information about undercover agents or police informers or about the organisation and tactics of operational-search measures may not be submitted to the judge and are therefore excluded from the court's scope of review. The Court considers that the failure to disclose the relevant information to the courts deprives them of the power to assess whether there is a sufficient factual basis to suspect the person in respect of whom operational-search measures are requested of a criminal offence or of activities endangering national, military, economic or ecological security. The Court has earlier found that there are techniques that can be employed which both accommodate legitimate security concerns about the nature and sources of intelligence information and yet accord the individual a substantial measure of procedural justice.

262. Furthermore, the Court observes that in Russia the judges are not instructed, either by the CCrP or by the OSAA, to verify the existence of a "reasonable suspicion" against the person concerned or to apply the "necessity" and "proportionality" test". At the same time... The Constitutional Court has therefore recommended, in substance, that when examining interception authorisation requests Russian courts should verify the existence of a reasonable suspicion against the person concerned and should authorise interception only if it meets the requirements of necessity and proportionality.

263. However, the Court observes that the domestic law does not explicitly require the courts of general jurisdiction to follow the Constitutional Court's opinion as to how a legislative provision should be interpreted if such opinion has been expressed in a decision rather than a judgment. Indeed, the materials submitted by the applicant show that the domestic courts do not always follow the above- mentioned recommendations of the Constitutional Court, all of which were contained in decisions rather than in judgments. Thus, it transpires from the analytical notes issued by District Courts that interception requests are often not accompanied by any supporting materials, that the judges of these District Courts never request the interception agency to submit such materials and that a mere reference to the existence of information about a criminal offence or activities endangering national, military, economic or ecological security is considered to be sufficient for the authorisation to be granted. An interception request is rejected only if it is not signed by a competent person, contains no reference to the offence in connection with which interception is to be ordered, or concerns a criminal offence in respect of which interception is not permitted under domestic law. Thus,

the analytical notes issued by District Courts, taken together with the statistical information for the period from 2009 to 2013 provided by the applicant, indicate that in their everyday practice Russian courts do not verify whether there is a "reasonable suspicion" against the person concerned and do not apply the "necessity" and "proportionality" test.

264. Lastly, as regards the content of the interception authorisation, it must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information.

265. The Court observes that the CCrP requires that a request for interception authorisation must clearly mention a specific person whose communications are to be intercepted, as well as the duration of the interception measure. By contrast, the OSAA does not contain any requirements either with regard to the content of the request for interception or to the content of the interception authorisation. As a result, courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed. Some authorisations do not mention the duration for which interception is authorised. The Court considers that such authorisations, which are not clearly prohibited by the OSAA, grant a very wide discretion to the law-enforcement authorities as to which communications to intercept, and for how long.

266. The Court further notes that in cases of urgency it is possible to intercept communications without prior judicial authorisation for up to forty-eight hours. A judge must be informed of any such case within twenty-four hours from the commencement of the interception. If no judicial authorisation has been issued within forty-eight hours, the interception must be stopped immediately. The Court has already examined the "urgency" procedure provided for in Bulgarian law and found that it was compatible with the Convention. However, in contrast to the Bulgarian provision, the Russian "urgent procedure" does not provide for sufficient safeguards to ensure that it is used sparingly and only in duly justified cases... The domestic law does not limit the use of the urgency procedure to cases involving an immediate serious danger to national, military, economic or ecological security. It leaves the authorities an unlimited degree of discretion in determining in which situations it is justified to use the non-judicial urgent procedure, thereby creating possibilities for abusive recourse to it. Furthermore, although Russian law requires that a judge be immediately informed of each instance of urgent interception, his or her power is limited to authorising the extension of the interception measure beyond forty-eight hours. He or she has no power to assess whether the use of the urgent procedure was justified or to decide whether the material obtained during the previous forty-eight hours is to be kept or destroyed. Russian law does therefore not provide for an effective judicial review of the urgency procedure.

267. In view of the above considerations the Court considers that the authorisation procedures provided for by Russian law are not capable of ensuring that secret surveillance measures are not ordered haphazardly, irregularly or without due and proper consideration.

268. The Court takes note of the applicant's argument that the security services and the police have the technical means to intercept mobile telephone communications without obtaining judicial authorisation, as they have direct access to all communications and as their ability to intercept the communications of a particular individual or individuals is not conditional on providing an interception authorisation to the communications service provider.

269. The Court considers that the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception... in particular the addendums to Order No.70, communications service providers must install equipment giving the law-enforcement authorities direct access to all mobile telephone communications of all users. The communications service providers also have an obligation under Order no. 538 to create databases storing information about all subscribers, and the services provided to them, for three years; the secret services have direct remote access to those databases. The law-enforcement authorities thus have direct access to all mobile telephone communications and related communications data.

270. The Court considers that the manner in which the system of secret surveillance operates in Russia gives the security services and the police technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation. Although the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system, the Court considers that a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great."

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

"73. ...Moreover, particularly in this context the Court notes the absence of prior judicial authorisation for interceptions... This safeguard would serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of "persons concerned identified ... as a range of persons" by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case. It is only in this way that the need for safeguards to ensure that emergency measures are used sparingly and only in duly justified cases can be satisfied...

79. It is in this context that the external, preferably judicial, a posteriori control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance, by reinforcing citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained. The significance of this control cannot be overestimated in view of the magnitude of the pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks. The Court notes the lack of such a control mechanism in Hungary.

80. The Court concedes that by the nature of contemporary terrorist threats there can be situations of emergency in which the mandatory application of judicial authorisation is not feasible, would be counterproductive for lack of special knowledge or would simply amount to wasting precious time. This is especially true in the present-day upheaval caused by terrorist attacks experienced throughout the world and in Europe, all too often involving important

losses of life, producing numerous casualties and significant material damage, which inevitably disseminate a feeling of insecurity amongst citizens...

81. Furthermore, where situations of extreme urgency are concerned, the law contains a provision under which the director of the service may himself authorise secret surveillance measures for a maximum of 72 hours. For the Court, this exceptional power should be sufficient to address any situations in which external, judicial control would run the risk of losing precious time. Such measures must however be subject to a post factum review, which is required, as a rule, in cases where the surveillance was authorised ex ante by a non-judicial authority."

European Commission For Democracy Through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006 (7 April 2015)

"16. Another safeguard is a definition of the categories of people liable to have their communications intercepted. The power to contact chain (i.e. identify people in contact with each other) should be framed narrowly contact chaining of metadata should normally only be possible for people suspected of actual involvement in particularly seriously offences, such as terrorism. If the legislature nonetheless considers that such a widely framed contact-chaining power is necessary, then this must be subject to procedural controls and strong oversight.

42. All of these methods of surveillance used by internal security agencies are "targeted" in the sense that they begin with the hypothesis that a person, or persons, have committed, are committing, or are planning the commission of a security offence, or, for states which do not limit the mandate of the security agency to investigating offences, are engaged in conduct threatening national security. All these methods interfere with Article 8 ECHR and other human rights and so a threshold is set in the law for initiating surveillance: there must be concrete facts indicating the criminal offence/security-threatening conduct, and the investigators must have "probable cause", "reasonable suspicion" or satisfy some similar test.

51. Strategic surveillance thus differs in a number of ways from surveillance in law enforcement or more traditional internal security operations. It does not necessarily start with a suspicion against a particular person or persons. It can instead be proactive: finding a danger rather than investigating a known danger. Herein lay both the value it can have for security operations, and the risks it can pose for individual rights. Prosecution is not the main purpose of gathering intelligence. The intelligence is, however, stored and used in a number of ways which can affect human rights. Nonetheless, despite the differences between targeted and strategic surveillance, it is apparent that at various stages in the proceedings, safeguards can exist, or can be created, to weigh privacy and other human rights against effectiveness in investigation of crime or threats against national security, to reduce the impact on human rights and to limit the scope for abuse of power."

ii. Effective Oversight (extended)

Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014)

"Reform the current oversight system of surveillance activities to ensure its effectiveness, including by providing for judicial involvement in the authorization or monitoring of surveillance measures, and considering the establishment of strong and independent oversight mandates with a view to preventing abuses"

Concluding Observations on the Initial Periodic Report of Malawi, Human Rights Committee, U.N. Doc. CCPR/C/MWI/CO/1/Add.1 (19 August 2014)

"20. The Committee is concerned that the legal provision expanding the authorization of searches without warrant is still in force... The State Party should: (a) Reconsider repealing section 35 of the Police Act in order to prevent arbitrary searches and interference with liberty and privacy."

Concluding Observations on the Seventh Periodic Report of the Russian Federation, Human Rights Committee, U.N. Doc. CCPR/C/RUS/CO/7 (28 April 2015)

"13. The Committee regrets the lack of clarity as to whether the 2006 Federal Counter-Terrorism Act: ...(c) provides for independent review of counter-terrorism activities undertaken by the executive, including with regard to monitoring telephone, electronic and postal communications. ...The State party should also ensure that its counter-terrorism legislation provides for an independent mechanism to review counter-terrorism activities undertaken by the executive."

Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, U.N. Doc CCPR/C/CAN/CO/6 (13 August 2015)

"10. ...The Committee is also concerned about the lack of adequate and effective oversight mechanisms to review activities of security and intelligence agencies and the lack of resources and power of existing mechanisms to monitor such activities... The State Party should… (d) Establish oversight mechanisms over security and intelligence agencies that are effective and adequate and provide them appropriate powers as well as sufficient resources to carry out their mandate; (e) Provide for judicial involvements in the authorization of surveillance measures..."

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (17 August 2015)

"24. The State Party should: ...(c) Ensure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for judicial involvement in the authorization of such measures in all cases, and by considering the establishment of strong and independent oversight mandates with a view to preventing abuses."

Concluding observations on the fifth periodic report of France, Human Rights Committee, U.N. Doc. CCPR/C/FRA/CO/5 (17 August 2015)

"12. ...It should also ensure the effectiveness and independence of a monitoring system for surveillance activities, in particular by making provision for the judiciary to take part in the authorization and monitoring of surveillance measures."

Concluding Observations on the Fourth Periodic Report of Rwanda, Human Rights Committee, U.N. Doc. CCPR/C/RWA/CO/4 (2 May 2016)

"35. The Committee is concerned that Law No. 60/2013 permits the interception of communications without prior authorization of a judge.

36. The State party should take legislative and other measures necessary to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity... It should also ensure the effectiveness and independence of a monitoring system for such interception, in particular by providing for the judiciary to take part in the authorization and monitoring of the interception."

Concluding Observations on the Initial Report of Pakistan, Human Rights Committee, U.N. Doc. CCPR/C/PAK/CO/1 (27 July 2017)

"35. While noting the State party's view that the Prevention of Electronic Crimes Act 2016 complies with the Convention on Cybercrime, the Committee is concerned that the Act provides for (a) overbroad powers to the Pakistan Telecommunication Authority and the authorized officers without sufficient independent judicial oversight mechanisms...

36. The State party should review its legislation on data collection and surveillance, in particular, the Prevention of Electronic Crimes Act 2016, to bring it in line with its obligations under the Covenant. It should also establish independent oversight mechanisms on the implementation of the Act, including judicial review of surveillance activity..."

Concluding Observations on the Second Periodic Report of Honduras, Human Rights Committee, U.N. Doc. CCPR/C/HND/CO/2 (27 July 2017) (translated from the original Spanish)

"38. The Committee is concerned about allegations regarding the frequent application of the Special Law on the Interception of Private Communications, which entails extensive monitoring of private communications. It also concerned about [...] the lack of adequate monitoring mechanisms to continuously review the application of the Special Law; And the difficulty of obtaining judicial redress from victims of unlawful surveillance.

39. The State party should [...] ensure that the implementation of the Special Law on the Interception of Private Communications is subject to continuous and adequate monitoring by means of an independent monitoring mechanism which provides victims with adequate remedies."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/HRC/13/37 (28 December 2009)

"51. Surveillance systems require effective oversight to minimize harm and abuses. Where safeguard 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...

53. ...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."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (17 April 2013)

"93. States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance communications."

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"38. Judicial involvement that meets international standards relating to independence, impartiality and transparency can help to make it more likely that the overall statutory regime will meet the minimum standards that international human rights law requires. At the same time, judicial involvement in oversight should not be viewed as a panacea; in several countries, judicial warranting or review of the digital surveillance activities of intelligence and/or law enforcement agencies have amounted effectively to an exercise in rubber-stamping. Attention is therefore turning increasingly towards mixed models of administrative, judicial and parliamentary oversight... There is particular interest in the creation of "public interest advocacy" positions within surveillance authorization processes. Given the growing role of third parties, such as Internet service providers, consideration may also need to be given to allowing such parties to participate in the authorization of surveillance measures affecting their interests or allowing them to challenge existing measures. The utility of independent advice, monitoring and/or review to help to ensure strict scrutiny of measures imposed under a statutory surveillance regime has been highlighted positively in relevant jurisprudence. Parliamentary committees also can play an important role; however, they may also lack the independence, resources or willingness to discover abuse, and may be subject to regulatory capture. Jurisprudence at the regional level has emphasized the utility of an entirely independent oversight body, particularly to monitor the execution of approved surveillance measures. In 2009, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism suggested, therefore, that "there must be no secret surveillance system that is not under review of an independent oversight body and all interferences must be authorized through an independent body."

Klass and Others v. Germany, App. No. 5029/71, European Court of Human Rights, Judgment (6 September 1978)

"54. The Government maintains that Article 8 para. 2 (art. 8-2) does not require judicial control of secret surveillance and that the system of review established under the G 10 does effectively protect the rights of the individual. The applicants, on the other hand, qualify this system as a "form of political control", inadequate in comparison with the principle of judicial control which ought to prevail. It therefore has to be determined whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" resulting from the contested legislation to what is "necessary in a democratic society".

55. Review of surveillance may intervene at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the

very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 para. 2 (art. 8-2), are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.

56. Within the system of surveillance established by the G 10, judicial control was excluded, being replaced by an initial control effected by an official qualified for judicial office and by the control provided by the Parliamentary Board and the G 10 Commission. The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge. Nevertheless, having regard to the nature of the supervisory and other safeguards provided for by the G 10, the Court concludes that the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society. The Parliamentary Board and the G 10 Commission are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character is reflected in the balanced membership of the Parliamentary Board. The opposition is represented on this body and is therefore able to participate in the control of the measures ordered by the competent Minister who is responsible to the Bundestag. The two supervisory bodies may, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling."

Rotaru v. Romania, App. No. 28341/95, European Court of Human Rights, Judgment (4 May 2000)

"59. The Court must also be satisfied that there exist adequate and effective safeguards against abuse, since a system of secret surveillance designed to protect national security entails the risk of undermining or even destroying democracy on the ground of defending it. In order for systems of secret surveillance to be compatible with Article 8 of the Convention, they must contain safeguards established by law which apply to the supervision of the relevant services' activities. Supervision procedures must follow the values of a democratic society as faithfully as possible, in particular the rule of law, which is expressly referred to in the Preamble to the Convention. The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure."

Iordachi and Others v. Moldova, App. No. 25198/02, European Court of Human Rights, Judgment (24 September 2009)

"40. Moreover, the Court recalls that in Dumitru Popescu v. Romania the Court expressed the view that the body issuing authorisations for interception should be independent and that there must be either judicial control or control by an independent body over the issuing body's activity...

47. ...it would appear that the investigating judge plays a very limited role. According to Article 41 of the Code of Criminal Procedure, his role is to issue interception warrants. According to Article 136 of the same Code, the investigating judge is also entitled to store "the original copies of the tapes along with the complete written transcript ... in a special place in a sealed envelope" and to adopt "a decision regarding the destruction of records which are not important for the criminal case". However, the law makes no provision for acquainting the investigating judge with the results of the surveillance and does not require him or her to review whether the requirements of the law have been complied with. On the contrary, section 19 of the Law on Operational Investigative Activities appears to place such supervision duties on the "Prosecutor General, his or her deputy, and the municipal and county prosecutors"...

48. Another point which deserves to be mentioned in this connection is the apparent lack of regulations specifying with an appropriate degree of precision the manner of screening the intelligence obtained through surveillance, or the procedures for preserving its integrity and confidentiality and the procedures for its destruction.

49. The Court further notes that overall control of the system of secret surveillance is entrusted to the Parliament which exercises it through a specialised commission. However, the manner in which the Parliament effects its control is not set out in the law and the Court has not been presented with any evidence indicating that there is a procedure in place which governs the Parliament's activity in this connection...

51. The Court notes further that in 2007 the Moldovan courts authorised virtually all the requests for interception made by the prosecuting authorities. Since this is an uncommonly high number of authorisations, the Court considers it necessary to stress that telephone tapping is a very serious interference with a person's rights and that only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorising it. The Court notes that the Moldovan legislation does not elaborate on the degree of reasonableness of the suspicion against a person for the purpose of authorising an interception. Nor does it contain safeguards other than the one provided for in section 6(1), namely that interception should take place only when it is otherwise impossible to achieve the aims. This, in the Court's opinion, is a matter of concern when looked at against the very high percentage of authorisations issued by investigating judges. For the Court, this could reasonably be taken to indicate that the investigating judges do not address themselves to the existence of compelling justification for authorising measures of secret surveillance.

52. ...In this connection, the Court notes the statistical information contained in the letter of the Head of the President's Office of the Supreme Court of Justice. According to that information, in 2005 over 2,500 interception warrants were issued, in 2006 some 1,900 were issued and over 2,300 warrants were issued in 2007. These figures show that the system of secret surveillance in Moldova is, to say the least, overused, which may in part be due to the inadequacy of the safeguards contained in the law."

Kennedy v. The United Kingdom, App. No. 26839/05, European Court of Human Rights, Judgment (18 May 2010)

"166. As regards supervision of the RIPA regime, the Court observes that apart from the periodic review of interception warrants and materials by intercepting agencies and, where appropriate, the Secretary of State, the Interception of Communications Commissioner established under RIPA is tasked with overseeing the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases. He has described his role as one of protecting members of the public from unlawful intrusion into their private lives, of assisting the intercepting agencies in their work, of ensuring that proper safeguards are in place to protect the public and of advising the Government and approving the safeguard documents. The Court notes that the Commissioner is independent of the executive and the legislature and is a person who holds or has held high judicial office. He reports annually to the Prime Minister and his report is a public document (subject to the non-disclosure of confidential annexes) which is laid before Parliament. In undertaking his review of surveillance practices, he has access to all relevant documents, including closed materials and all those involved in interception activities have a duty to disclose to him any material he requires. The obligation on intercepting agencies to keep records ensures that the Commissioner has effective access to details of surveillance activities undertaken. The Court further notes that, in practice, the Commissioner reviews, provides advice on and approves the section 15 arrangements. The Court considers that the Commissioner's role in ensuring that the provisions of RIPA and the Code are observed and applied correctly is of particular value and his biannual review of a random selection of specific cases in which interception has been authorised provides an important control of the activities of the intercepting agencies and of the Secretary of State himself.

167. The Court recalls that it has previously indicated that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge. In the present case, the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers. In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant. In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid. The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom

168. Finally, the Court observes that the reports of the Commissioner scrutinise any errors which have occurred in the operation of the legislation. In his 2007 report, the Commissioner commented that none of the breaches or errors identified were deliberate and that, where interception had, as a consequence of human or technical error, unlawfully taken place, any intercept material was destroyed as soon as the error was discovered. There is therefore no evidence that any deliberate abuse of interception powers is taking place.

169. In the circumstances, the Court considers that the domestic law on interception of internal communications together with the clarifications brought by the publication of the Code indicate with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of intercept material collected. The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the surveillance regime. On the contrary, the various reports of the Commissioner have highlighted the diligence with which the authorities implement RIPA and correct any technical or human errors which accidentally occur. Having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, insofar as they may have been applied to the applicant in the circumstances outlined in the present case, are justified under Article 8 § 2."

Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015)

"249. ...the Court does not lose sight of the fact that prior judicial authorisation for interceptions is required in Russia. Such judicial authorisation may serve to limit the law-enforcement authorities' discretion in interpreting the broad terms of "a person who may have information about a criminal offence", "a person who may have information relevant to the criminal case", and "events or activities endangering Russia's national, military, economic or ecological security" by following an established judicial interpretation of the terms or an established practice to verify whether sufficient reasons for intercepting a specific individual's communications exist in each case. The Court accepts that the requirement of prior judicial authorisation constitutes an important safeguard against arbitrariness. The effectiveness of that safeguard will be examined below.

250. The Court has held that it is not unreasonable to leave the overall duration of interception to the discretion of the relevant domestic authorities which have competence to issue and renew interception warrants, provided that adequate safeguards exist, such as a clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled…

273. As regards supervision of interceptions carried out on the basis of proper judicial authorisations, the Court will examine whether the supervision arrangements existing in Russia are capable of ensuring that the statutory requirements relating to the implementation of the surveillance measures, the storage, access to, use, processing, communication and destruction of intercept material are routinely respected.

274. A court which has granted authorisation for interception has no competence to supervise its implementation. It is not informed of the results of the interceptions and has no power to review whether the requirements of the decision granting authorisation were complied with. Nor do Russian courts in general have competence to carry out the overall supervision of interceptions. Judicial supervision is limited to the initial authorisation stage. Subsequent supervision is entrusted to the President, Parliament, the Government, the Prosecutor General and competent lower-level prosecutors.

275. The Court has earlier found that, although it is in principle desirable to entrust supervisory control to a judge, supervision by non- judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out

the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control.

276. As far as the President, Parliament and the Government are concerned, Russian law does not set out the manner in which they may supervise interceptions. There are no publicly available regulations or instructions describing the scope of their review, the conditions under which it may be carried out, the procedures for reviewing the surveillance measures or for remedying the breaches detected.

277. As regards supervision of interceptions by prosecutors, the Court observes that the national law sets out the scope of, and the procedures for, prosecutors' supervision of operational-search activities. It stipulates that prosecutors may carry out routine and ad hoc inspections of agencies performing operational-search activities and are entitled to study the relevant documents, including confidential ones. They may take measures to stop or remedy the detected breaches of law and to bring those responsible to liability. They must submit semi-annual reports detailing the results of the inspections to the Prosecutor General's Office. The Court accepts that a legal framework exists which provides, at least in theory, for some supervision by prosecutors of secret surveillance measures. It must be next examined whether the prosecutors are independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise effective and continuous control.

278. As to the independence requirement, in previous cases the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it found sufficiently independent the bodies composed of members of parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by parliament or by the Prime Minister. In contrast, a Minister of Internal Affairs – who not only was a political appointee and a member of the executive, but was directly involved in the commissioning of special means of surveillance – was found to be insufficiently independent. Similarly, a Prosecutor General and competent lower-level prosecutors were also found to be insufficiently independent.

279. In contrast to the supervisory bodies cited above, in Russia prosecutors are appointed and dismissed by the Prosecutor General after consultation with the regional executive authorities. This fact may raise doubts as to their independence from the executive.

280. Furthermore, it is essential that any role prosecutors have in the general protection of human rights does not give rise to any conflict of interest. The Court observes that prosecutor's offices do not specialise in supervision of interceptions. Such supervision is only one part of their broad and diversified functions, which include prosecution and supervision of criminal investigations. In the framework of their prosecuting functions, prosecutors give their approval to all interception requests lodged by investigators in the framework of criminal proceedings. This blending of functions within one prosecutor's office, with the same office giving approval to requests for interceptions and then supervising their implementation, may also raise doubts as to the prosecutors' independence.

281. Turning now to the prosecutors' powers and competences, the Court notes that it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required. Russian law stipulates that prosecutors are entitled to study relevant documents, including confidential ones. It is however important to note that information about

the security services' undercover agents, and about the tactics, methods and means used by them, is outside the scope of prosecutors' supervision.

282. The supervisory body's powers with respect to any breaches detected are also an important element for the assessment of the effectiveness of its supervision. The Court is satisfied that prosecutors have certain powers with respect to the breaches detected by them. Thus, they may take measures to stop or remedy the detected breaches of law and to bring those responsible to liability. However, there is no specific provision requiring destruction of the unlawfully obtained intercept material.

283. The Court must also examine whether the supervisory body's activities are open to public scrutiny. In Russia, prosecutors must submit semi-annual reports detailing the results of the inspections to the Prosecutor General's Office. However, these reports concern all types of operational-search measures, amalgamated together, without interceptions being treated separately from other measures. Moreover, the reports contain only statistical information about the number of inspections of operational-search measures carried out and the number of breaches detected, without specifying the nature of the breaches or the measures taken to remedy them. It is also significant that the reports are confidential documents. They are not published or otherwise accessible to the public. It follows that in Russia supervision by prosecutors is conducted in a manner which is not open to public scrutiny and knowledge.

284. Lastly, the Court notes that it is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples. However, the Russian Government did not submit any inspection reports or decisions by prosecutors ordering the taking of measures to stop or remedy a detected breach of law. It follows that the Government did not demonstrate that prosecutors' supervision of secret surveillance measures is effective in practice. The Court also takes note in this connection of the documents submitted by the applicant illustrating prosecutors' inability to obtain access to classified materials relating to interceptions. That example also raises doubts as to the effectiveness of supervision by prosecutors in practice.

285. In view of the defects identified above, and taking into account the particular importance of supervision in a system where law-enforcement authorities have direct access to all communications, the Court considers that the prosecutors' supervision of interceptions as it is currently organised is not capable of providing adequate and effective guarantees against abuse."

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

"82. The Court notes at this juncture the liability of the executive to give account, in general terms rather than concerning any individual cases, of such operations to a parliamentary committee. However, it cannot identify any provisions in Hungarian legislation permitting a remedy granted by this procedure during the application of measures of secret surveillance to those who are subjected to secret surveillance but, by necessity, are kept unaware thereof. The Minister is under an obligation to present a general report, at least twice a year, to the responsible parliamentary committee about the functioning of national security services, which report, however, does not seem to be available to the public and by this appears to fall short of securing adequate safeguards in terms of public scrutiny. The committee is entitled, of its own motion, to request information from the Minister and the directors of the services about the

activities of the national security services. However, the Court is not persuaded that this scrutiny is able to provide redress to any individual grievances caused by secret surveillance or to control effectively, that is, in a manner with a bearing on the operations themselves, the daily functioning of the surveillance organs, especially since it does not appear that the committee has access in detail to relevant documents. The scope of their supervision is therefore limited.

85. In any event, the Court recalls that in Klass and Others a combination of oversight mechanisms, short of formal judicial control, was found acceptable in particular because of "an initial control effected by an official qualified for judicial office". However, the Hungarian scheme of authorisation does not involve any such official. The Hungarian Commissioner for Fundamental Rights has not been demonstrated to be a person who necessarily holds or has held a judicial office.

88. Lastly, the Court notes that is for the Government to illustrate the practical effectiveness of the supervision arrangements with appropriate examples. However, the Government were not able to do so in the instant case.

89. In total sum, the Court is not convinced that the Hungarian legislation on "section 7/E (3) surveillance" provides safeguards sufficiently precise, effective and comprehensive on the ordering, execution and potential redressing of such measures. Given that the scope of the measures could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity, that new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones, the Court concludes that there has been a violation of Article 8 of the Convention."

Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services, Commissioner's Recommendations (May 2015)

"1. Establish or designate one or more bodies that are fully independent from the executive and the security services to oversee all aspects of security service regulations, policies, operations and administration...

3. Ensure that all aspects and phases of the collection (regardless of its method of collection or provenance), processing, storage, sharing, minimisation and deletion of personal data by security services are subject to oversight by at least one institution that is external to the security services and the executive.

4. Ensure that the oversight of security services focuses not only on the lawfulness of security service activities that restrict the right to privacy and family life but also the rights to freedom of expression, assembly, association and religion, thought and conscience.

5. Mandate oversight bodies to scrutinise the human rights compliance of security service co-operation with foreign bodies, including co-operation through the exchange of information, joint operations and the provision of equipment and training. External oversight of security service co-operation with foreign bodies should include but not be limited to examining: (a) ministerial directives and internal regulations relating to international intelligence co-

operation; (b) human rights risk assessment and risk-management processes relating to relationships with specifc foreign security services and to specifc instances of operational co-operation; (c) outgoing personal data and any caveats (conditions) attached thereto; (d) security service requests made to foreign partners: (i) for information on specifc persons; and (ii) to place specifc persons under surveillance; (e) intelligence co-operation agreements; (f) joint surveillance operations and programmes undertaken with foreign partners.

6. Require that security services obtain authorisation from a body that is independent from the security services and the executive, both in law and in practice, before engaging in any of the following activities either directly or through/in collaboration with private sector entities: (a) conducting untargeted bulk surveillance measures regardless of the methods or technology used or the type of communications targeted; (b) using selectors or key words to extract data from information collected through bulk surveillance, particularly when these selectors relate to identifable persons; (c) collecting communications/metadata directly or accessing it through requests made to third parties, including private companies; (d) accessing personal data held by other state bodies; (e) undertaking computer network exploitation.

7. Ensure that, where security services engage in computer network exploitation, these activities are subject to the same level of external oversight as is required for surveillance measures that have equivalent human rights implications.

8. Consider the introduction of security-cleared public interest advocates into surveillance authorisation processes, including both targeted and untargeted surveillance measures, to represent the interests of would-be targets of surveillance.

9. Consider how surveillance authorisation processes can be kept under ex post facto review by an independent body that is empowered to examine decisions taken by the authorising body.

10. Create or designate an external oversight body to receive and investigate complaints relating to all aspects of security service activity. Where such bodies are only empowered to issue non-binding recommendations, member states must ensure that complainants also have recourse to another institution that can provide remedies that are effective both in law and in practice.

11. Give an external oversight body the power to quash surveillance warrants and discontinue surveillance measures undertaken without the need for a warrant when such activities are deemed to have been unlawful, as well as the power to require the deletion of any information obtained from the use of such measures.

12. Ensure that the procedures of any institution tasked with adjudicating on complaints relating to matters that have been revealed to a complainant or otherwise made public comply with due process standards under European human rights law."

Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection, pp. 10-11 (5 June 2015)

"States should establish or designate one or more bodies that are fully independent from the executive and the security services to oversee all aspects of security service regulations, policies, operations, data collection and administration, and ensure that their systems for the oversight of security services comply with human rights requirements...

Independent ex ante authorisation should be extended to: untargeted bulk collection of information; the collection of and access to communications data (including when held by the private sector); and, potentially, computer network exploitation. The process by which intrusive measures are authorised or re-authorised should itself be subject to scrutiny. Given the difficulties that may arise when seeking to evaluate judicial decisions on the authorisation of intrusive measures, consideration may be given to quasi-judicial models.

States should consider the introduction of security-cleared public interest advocates into surveillance authorisation processes, create or designate an independent, external oversight body to receive and investigate complaints relating to all aspects of security service activity, and give an external oversight body the power to quash surveillance measures when such activities are deemed to have been unlawful. Independent, external bodies responsible for scrutinising security services should publish public versions of their periodic and investigation reports...

An independent assessment of the use and impact of individual information databases must be carried out in order to ensure that they are necessary and proportionate. The use of data collected through telecommunication surveillance or other forms of undercover investigations should be strictly limited to the purpose of investigating serious crimes. Surveillance activities should be authorised by a judge, set out strict limits on its duration, as well as rules on the disclosure and destruction of surveillance data, and provide for ex post remedies to all individuals concerned."

European Commission For Democracy Through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006 (7 April 2015)

"20. Two very significant stages in the signals intelligence process where safeguards must apply are the authorization and follow-up (oversight) processes. That the latter must be performed by an independent, external body is clear from the ECtHR's case law. The question which arises here is whether even the authorization process should be independent.

21. Internal and governmental controls as part of overall accountability systems. For a number of reasons, It has been particularly tempting to rely primarily on internal controls in the area of strategic surveillance, but they are insufficient. Generally speaking, external oversight over signals intelligence needs to be strengthened considerably.

22. Parliamentary accountability. There are a number of reasons why parliamentary supervision of strategic surveillance is problematic. First, the technical sophistication of signals intelligence makes it difficult for parliamentarians to supervise without the aid of technical experts. Second, the general problem of parliamentarians finding sufficient time for oversight along with all their other duties is particularly acute as regards strategic surveillance, where for controlling the dynamic process of refining the selectors (as opposed to a post-hoc scrutiny), some form of standing body is necessary. Thirdly, the high degree of network cooperation between certain signals intelligence agencies means an added reluctance to admit in parliamentary oversight, which can thus affect not simply one's own agencies, but also those of one's allies. In some states the doctrine of parliamentary privilege means that parliamentary committees cannot be security-screened, adding to an already-existing fear of leaks. The other,

crucial, factor is that strategic surveillance involves an interference with individual rights. Supervision of such measures has traditionally been a matter for the judiciary. The constitutional principle of separation of powers can make it problematic for a parliamentary body to play such a quasi-judicial role.

23. A decision to use particular selectors, resembles, at least in some ways, a decision to authorize targeted surveillance. As such, it can be taken by a judicial body. As the decision involves considerable policy elements, knowledge of intelligence techniques and foreign policy are also desirable. Finding a group of people who combine all three types of competence is not easy, even for a large state. Thus, it is easier to create a hybrid body of judges and other experts. As regards follow-up (oversight) it is necessary to oversee decisions made by automated systems for deleting irrelevant data, as well as decisions by human analysts to keep the personal information collected, and to transfer it to other domestic and foreign agencies. This type of oversight is of a "data protection" character, most suitably assigned to an independent, expert administrative body. Neither of these types of decision is "political" in nature. What, by contrast, is more "political" is the prior decision taken, that somebody, or something, is of sufficient importance to national security to need intelligence about. This is the type of decision which would benefit from a (closed) discussion in a political body, where different spectrums of opinion are represented. Another type of policy-oriented issue is deciding the general rules regarding who, and under what circumstances, signals intelligence can be exchanged with other signals intelligence organisations. A third is making a general evaluation of the overall effectiveness and efficacy of signals intelligence measures. A fourth role for a political body is to engage in a continuous dialogue with whatever expert oversight body is established.

24. Judicial authorization. A system of authorization needs to be complemented by some form of follow-up control that conditions are being complied with. This is necessary both because the process of refining selectors is dynamic and highly technical and because judges do not tend to see the results of the signals intelligence operations as these seldom lead to prosecutions. Thus the safeguards applying to a subsequent criminal trial do not become applicable."

Maximillian Schrems v. Data Protection Commissioner (C-362/14), Court of Justice of the European Union, Grand Chamber, Judgment (6 October 2015)

"39. It is apparent from Article 1 of Directive 95/46 and recitals 2 and 10 in its preamble that that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms...

40. As regards the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, it should be noted that Article 28(1) of Directive 95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. In addition, that requirement derives from the primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU.

41. The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities. The establishment in Member States of independent supervisory authorities is therefore, as stated in recital 62 in the preamble to Directive 95/46, an essential component of the protection of individuals with regard to the processing of personal data.

42. In order to guarantee that protection, the national supervisory authorities must, in particular, ensure a fair balance between, on the one hand, observance of the fundamental right to privacy and, on the other hand, the interests requiring free movement of personal data.

43. The national supervisory authorities have a wide range of powers for that purpose. Those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means to perform their duties, as stated in recital 63 in the preamble to the directive. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings."

Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016)

"120. In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime...

123. In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data."

Draft agreement between Canada and the European Union on the Transfer of Passenger Name Record data (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)

"229. In accordance with the settled case-law of the Court, the guarantee of the independence of [a] supervisory authority [...] is intended to ensure the effectiveness and reliability of the monitoring of compliance with the rules concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. The

establishment of an independent supervisory authority is therefore an essential component of the protection of individuals with regard to the processing of personal data."

Garcia v. Peru, Inter-American Court of Human Rights, Case 11.006, Report No. 1/95, OEA/Ser.L/V/II.88, The Merits (17 February 1995)

"Article 11 of the American Convention on Human Rights protects the right to privacy and stipulates that no one may be the object of arbitrary or abusive interference in his private life or family...

The guarantee of the inviolability of the domicile and of private papers must give way when there is a well-substantiated search warrant issued by a competent judicial authority, spelling out the reasons for the measure being adopted and specifying the place to be searched and the objects that will be seized.

The 1979 Constitution of Peru stipulated the inviolability of domicile and of private papers except when an order has been issued by a competent judicial authority authorizing the search, explaining its reasons and, where appropriate, authorizing the seizure of private papers, while respecting the guarantees stipulated by law.

Based on these concepts, the Commission concludes that the warrantless search of Dr. García's home and the seizure of private family papers - actions committed by Peruvian Army soldiers - were committed in complete disregard of the procedural requirements stipulated in the Constitution. The violation of those requirements indicates that the Government of Peru failed to guarantee to Dr. Alan García and to his family the full exercise of their right to privacy."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"164. ... the Special Rapporteurs have already underscored the need for effective controls to ensure that online surveillance programs are designed and implemented taking account of all of the rights at stake, including the procedural guarantees.

165. In light of the above, decisions to undertake surveillance activities that invade the privacy of individuals must be authorized by independent judicial authorities, who must state why the measure is appropriate for the accomplishment of the objectives pursued in the specific case; whether it is sufficiently restricted so as not to infringe upon the right in question more than necessary; and whether it is proportionate in relation to the interests pursued. In this respect, the European Court of Human Rights has held that "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge." States must ensure that the judicial authority is specialized and competent to make decisions on the legality of the communications surveillance, the technologies used, and its impact on the sphere of rights that could be involved."

iii. Data Retention (extended)

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/71/199 (19 December 2016)

"Expressing concern that individuals often do not provide their free, explicit, and informed consent to the sale or multiple resale of their personal data, as the collecting, processing and sharing of personal data, including sensitive data, have increased significantly in the digital age...

Noting also the increasing capabilities of business enterprises to collect, process and use personal data can pose a risk to the enjoyment of the right to privacy in the digital age,

Welcoming measures taken by business enterprises, on a voluntary basis, to provide transparency to their users about their policies regarding requests by State authorities for access to user data and information."

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (17 August 2015)

"24. The State Party Should: …(d) Revise the Data Retention and Investigatory Powers Act 2014 with a view to ensuring that access to communications data is limited to the extent strictly necessary for prosecution of the most serious crimes and is dependent upon prior judicial authorization."

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1 (27 April 2016)

"42. [The Committee] is also concerned about the wide scope of the data retention regime under the [2002 Regulation of Interception of Communications and Provision of Communication-Related Information Act]...

43. The State Party should... consider revoking or limiting the requirement for mandatory retention of data by third parties..."

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6 (28 March 2017)

"36. ...[The Committee is concerned] that the Anti-Terrorism Decree and Law no. 21/2016 ("Decreto Mille Proroghe") compel telecommunication providers to retain data beyond the period allowed by Article 132 of the Personal Data Protection Code, and accessing such data by the authorities is not subject to authorization from a judicial authority...

37. The State party should review the regime regulating the interception of personal communications, hacking of digital devices and the retention of communications data with a view to ensuring (a) that such activities conform with its obligations under article 17 including with the principles of legality, proportionality and necessity, (b) that robust independent oversight systems over surveillance, interception and hacking, including by providing for judicial involvement in the authorization of such measures in all cases and affording persons affected with effective remedies in cases of abuse, including, where possible, an ex post notification that they were subject to measures of surveillance or hacking."

Concluding Observations on the Initial Report of Pakistan, Human Rights Committee, U.N. Doc. CCPR/C/PAK/CO/1 (27 July 2017)

"35. While noting the State party's view that the Prevention of Electronic Crimes Act 2016 complies with the Convention on Cybercrime, the Committee is concerned that the Act provides for... (b) mandatory mass retention of traffic data by service providers for a minimum of one year, (c) unduly restrictive licensing requirements of service providers...

36. The State party should review its legislation on data collection and surveillance, in particular, the Prevention of Electronic Crimes Act 2016, to bring it in line with its obligations under the Covenant. It should… review all licensing requirements which impose obligations on network service providers to engage in communication surveillance, particularly in relation to indiscriminate data retention; and ensure that surveillance activities comply with its obligations under the Covenant. It should further adopt a comprehensive data protection law in line with international standards."

Concluding Observations on the Fourth Periodic Report of Switzerland, Human Rights Committee, U.N. Doc. CCPR/C/CHE/CO/4 (27 July 2017) (translated from the original French)

"46. While noting the human rights safeguards measures introduced in the Federal Intelligence Act of 25 September 2016, the Committee is concerned that the Act gives very intrusive surveillance powers to the Intelligence Services of the Confederation on the basis of narrowly defined objectives, such as the national interests referred to in Article 3. It is also concerned about the absence of specific time limits for the retention of data.

47. The State party should take all necessary measures to ensure that its monitoring activities are in conformity with the obligations under the Covenant, in particular Article 17. In particular, measures will have to be taken to ensure that data retention periods Are strictly regulated."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (17 April 2013)

"95. States should ensure that communications data collected by corporate actors in the provision of communications services meets the highest standards of data protection."

Rotaru v. Romania, App. No. 28341/95, European Court of Human Rights, Judgment (4 May 2000)

"46. The Court points out that both the storing by a public authority of information relating to an individual's private life and the use of it and the refusal to allow an opportunity for it to be refuted amount to interference with the right to respect for private life secured in Article 8 § 1 of the Convention."

Kennedy v. The United Kingdom, App. No. 26839/05, European Court of Human Rights, Judgment (18 May 2010)

"162. As regards the procedure for examining, using and storing the data, the Government indicated in their submissions that, under RIPA, an intercepting agency could, in principle, listen to all intercept material collected. The Court recalls its conclusion in Liberty and Others, cited above, § 65, that the authorities' discretion to capture and listen to captured material was very wide. However, that case, unlike the present case, involved external communications, in respect of which data were captured indiscriminately. Contrary to the practice under the Interception of Communications Act 1985 concerning external communications, interception warrants for internal communications under RIPA relate to one person or one set of premises only, thereby limiting the scope of the authorities' discretion to intercept and listen to private communications. Moreover, any captured data which are not necessary for any of the authorised purposes must be destroyed.

163. As to the general safeguards which apply to the processing and communication of intercept material, the Court observes that section 15 RIPA imposes a duty on the Secretary of State to ensure that arrangements are in place to secure any data obtained from interception and contains specific provisions on communication of intercept material. Further details of the arrangements are provided by the Code. In particular, the Code strictly limits the number of persons to whom intercept material can be disclosed, imposing a requirement for the appropriate level of security clearance as well as a requirement to communicate data only where there is a "need to know". It further clarifies that only so much of the intercept material as the individual needs to know is to be disclosed and that where a summary of the material would suffice, then only a summary should be disclosed. The Code requires intercept material, as well as copies and summaries of such material, to be handled and stored securely to minimise the risk of threat or loss. In particular, it must be inaccessible to those without the necessary security clearance. A strict procedure for security vetting is in place. In the circumstances, the Court is satisfied that the provisions on processing and communication of intercept material provide adequate safeguards for the protection of data obtained.

64. As far as the destruction of intercept material is concerned, section 15(3) RIPA requires that the intercept material and any related communications data, as well as any copies made of the material or data, must be destroyed as soon as there are no longer any grounds for retaining them as necessary on section 5(3) grounds. The Code stipulates that intercept material must be reviewed at appropriate intervals to confirm that the justification for its retention remains valid.

65. The Code also requires intercepting agencies to keep detailed records of interception warrants for which they have applied, an obligation which the Court considers is particularly important in the context of the powers and duties of the Commissioner and the IPT."

Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015)

251. As regards the first safeguard, both the CCrP and the OSAA provide that interceptions may be authorised by a judge for a period not exceeding six months. There is therefore a clear indication in the domestic law of the period after which an interception authorisation will expire. Secondly, the conditions under which an authorisation can be renewed are also clearly set out in law. In particular, under both the CCrP and the OSAA a judge may extend interception for a maximum of six months at a time, after a fresh examination of all the relevant materials (id.). However, as regards the third safeguard concerning the circumstances in which the interception must be discontinued, the Court notes that the requirement to discontinue interception when no longer necessary is mentioned in the CCrP only. Regrettably, the OSAA

does not contain such a requirement (id.). In practice, this means that interceptions in the framework of criminal proceedings are attended by more safeguards than interceptions conducted outside such a framework, in particular in connection with "events or activities endangering national, military, economic or ecological security".

252. The Court concludes from the above that while Russian law contains clear rules on the duration and renewal of interceptions providing adequate safeguards against abuse, the OSAA provisions on discontinuation of the surveillance measures do not provide sufficient guarantees against arbitrary interference...

"253. Russian law stipulates that data collected as a result of secret surveillance measures constitute a State secret and are to be sealed and stored under conditions excluding any risk of unauthorised access. They may be disclosed to those State officials who genuinely need the data for the performance of their duties and have the appropriate level of security clearance. Steps must be taken to ensure that only the amount of information needed by the recipient to perform his or her duties is disclosed, and no more. The official responsible for ensuring that the data are securely stored and inaccessible to those without the necessary security clearance is clearly defined. Domestic law also sets out the conditions and procedures for communicating intercepted data containing information about a criminal offence to the prosecuting authorities. It describes, in particular, the requirements for their secure storage and the conditions for their use as evidence in criminal proceedings. The Court is satisfied that Russian law contains clear rules governing the storage, use and communication of intercepted data, making it possible to minimise the risk of unauthorised access or disclosure.

254. As far as the destruction of intercept material is concerned, domestic law provides that intercept material must be destroyed after six months of storage, if the person concerned has not been charged with a criminal offence. If the person has been charged with a criminal offence, the trial judge must make a decision, at the end of the criminal proceedings, on the further storage and destruction of the intercept material used in evidence.

255. As regards the cases where the person concerned has not been charged with a criminal offence, the Court is not convinced by the applicant's argument that Russian law permits storage of the intercept material beyond the statutory time-limit. It appears that the provision referred to by the applicant does not apply to the specific case of storage of data collected as a result of interception of communications. The Court considers the six-month storage time-limit set out in Russian law for such data reasonable. At the same time, it deplores the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they has been obtained. The automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8.

256. Furthermore, as regards the cases where the person has been charged with a criminal offence, the Court notes with concern that Russian law allows unlimited discretion to the trial judge to store or to destroy the data used in evidence after the end of the trial. Russian law does not give citizens any indication as to the circumstances in which the intercept material may be stored after the end of the trial. The Court therefore considers that the domestic law is not sufficiently clear on this point...

272. The Court notes at the outset that Order no. 70 requires that the equipment installed by the communications service providers does not record or log information about interceptions. The Court has found that an obligation on the intercepting agencies to keep records of

interceptions is particularly important to ensure that the supervisory body had effective access to details of surveillance activities undertaken. The prohibition on logging or recording interceptions set out in Russian law makes it impossible for the supervising authority to discover interceptions carried out without proper judicial authorisation. Combined with the law-enforcement authorities' technical ability, pursuant to the same Order no. 70, to intercept directly all communications, this provision renders any supervision arrangements incapable of detecting unlawful interceptions and therefore ineffective."

Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)

"39. So far as concerns the essence of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, it must be held that, even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.

40. Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that, without prejudice to the provisions adopted pursuant to Directives 95/46 and 2002/58, certain principles of data protection and data security must be respected by providers of publicly available electronic communications services or of public communications networks. According to those principles, Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data...

54. Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.

55. The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data.

56. As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article 3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.

57. In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data

without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.

58. Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.

59. Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.

60. Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.

61. Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.

62. In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.

63. Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

64. Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.

65. It follows from the above that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.

66. Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.

67. Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second subparagraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period."

Patrick Breyer v. Bundesrepublik Deutschland (C-582/14), Court of Justice of the European Union, Second Chamber, Judgment (19 October 2016)

"33. As a preliminary point, it must be noted that, in paragraph 51 of the judgment of 24 November 2011... the Court held essentially that the IP addresses of internet users were protected personal data because they allow users to be precisely identified.

34. However, that finding by the Court related to the situation in which the collection and identification of the IP addresses of internet users is carried out by internet service providers.

35. In the present case, the first question concerns the situation in which it is the online media services provider, namely the Federal Republic of Germany, which registers IP addresses of

the users of a website that it makes accessible to the public, without having the additional data necessary in order to identify those users.

36. Furthermore, it is common ground that the IP addresses to which the national court refers are 'dynamic' IP addresses, that is to say provisional addresses which are assigned for each internet connection and replaced when subsequent connections are made, and not 'static' IP addresses, which are invariable and allow continuous identification of the device connected to the network...

38. ...it must be noted, first of all, that it is common ground that a dynamic IP address does not constitute information relating to an 'identified natural person', since such an address does not directly reveal the identity of the natural person who owns the computer from which a website was accessed, or that of another person who might use that computer...

40. In that connection, it is clear from the wording of Article 2(a) of Directive 95/46 that an identifiable person is one who can be identified, directly or indirectly.

41. The use by the EU legislature of the word 'indirectly' suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified...

43. In so far as that recital refers to the means likely reasonably to be used by both the controller and by 'any other person', its wording suggests that, for information to be treated as 'personal data' within the meaning of Article 2(a) of that directive, it is not required that all the information enabling the identification of the data subject must be in the hands of one person...

45. However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject...

47. Although the referring court states in its order for reference that German law does not allow the internet service provider to transmit directly to the online media services provider the additional data necessary for the identification of the data subject, it seems however, subject to verifications to be made in that regard by the referring court that, in particular, in the event of cyber attacks legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to bring criminal proceedings.

48. Thus, it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored.

49. Having regard to all the foregoing considerations, the answer to the first question is that Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person...

62. Article 7(f) of that directive precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case. Thus, Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case.

63. As regards the processing of personal data of the users of online media websites, legislation, such as that at issue in the main proceedings, reduces the scope of the principle laid down in Article 7(f) of Directive 95/46 by excluding the possibility to balance the objective of ensuring the general operability of the online media against the interests or fundamental rights and freedoms of those users which, in accordance with that provision, calls for protection under Article 1(1) of that directive.

64. It follows from all of the foregoing considerations that the answer to the second question is that Article 7(f) of Directive 95/46 must be interpreted as meaning that it precludes the legislation of a Member State under which an online media services provider may collect and use personal data relating to a user of those service, without his consent, only in so far as the collection and use of that information are necessary to facilitate and charge for the specific use of those services by that user, even though the objective aiming to ensure the general operability of those services may justify the use of those data after consultation of those websites."

Draft agreement between Canada and the European Union on the Transfer of Passenger Name Record data (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)

"190. In order to ensure that the retention of the PNR data transferred, the access to that data by the Canadian authorities referred to in the envisaged agreement and the use of that data by those authorities is limited to what is strictly necessary, the envisaged agreement should, in accordance with the settled case-law of the Court [...], lay down clear and precise rules indicating in what circumstances and under which conditions those authorities may retain, have access to and use such data.

191. So far as the retention of personal data is concerned, it must be pointed out that the legislation in question must, inter alia, continue to satisfy objective criteria that establish a connection between the personal data to be retained and the objective pursued.

192. As regards the use, by an authority, of legitimately retained personal data, it should be recalled that the Court has held that EU legislation cannot be limited to requiring that access to such data should be for one of the objectives pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use.

202. ...it is essential that the use of retained PNR data, during the air passengers' stay in Canada, should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court, or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by the competent authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime.

205. as regards air passengers in respect of whom no such risk has been identified on their arrival in Canada and up to their departure from that non-member country, there would not appear to be, once they have left, a connection — even a merely indirect connection — between their PNR data and the objective pursued by the envisaged agreement which would justify that data being retained. The considerations put forward before the Court, inter alia, by the Council and the Commission regarding the average lifespan of international serious crime networks and the duration and complexity of investigations relating to those networks, do not justify the continued storage of the PNR data of all air passengers after their departure from Canada for the purposes of possibly accessing that data, regardless of whether there is any link with combating terrorism and serious transnational crime.

206. The continued storage of the PNR data of all air passengers after their departure from Canada is not therefore limited to what is strictly necessary...

210. Lastly, in so far as Article 9(2) of the envisaged agreement, which provides that Canada is to hold PNR data 'in a secure physical environment that is protected with access controls', means that that data has to be held in Canada, and in so far as Article 16(6) of that agreement, under which Canada is to destroy the PNR data at the end of the PNR data retention period, must be understood as requiring the irreversible destruction of that data, those provisions may be regarded as meeting the requirements as to clarity and precision."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"169. The service providers should be able to publicly disclose the procedures they use when they receive requests for information from government authorities, as well as information on at least the types of requests they receive and the number of requests. On this point, it bears noting that various Internet companies have adopted the practice of issuing transparency reports that disclose some aspects of the government requests for access to user information they receive...

173. In the interest of controlling foreign surveillance of personal data, some States have proposed establishing a legal obligation of forced localization with respect to some intermediaries. Forced localization is understood as the legal obligation of the owners of Internet sites, platforms, and services to store the data or information on national users locally (in-country) if they provide their services in that country. The forced localization of data may be a mechanism for the restriction of freedom of expression for various reasons. First, the forced localization of Internet intermediaries substantially reduces the supply of services and platforms that users can freely access. It is important to note that the freedom to choose which services and platforms to access is a prerogative of users in the exercise of their freedom of expression and cannot be restricted by governments without violating the unique nature of the Internet as a free, open, and decentralized medium. This opportunity to choose is essential in many States in which individuals are subjected to arbitrary interference in their privacy by the States. In such cases, the opportunity to choose the intermediaries that offer better security becomes a necessary condition for the uninhibited exercise of freedom of expression. In other words, the absence of adequate local laws or public policies for the protection of data could cause greater insecurity in the access to data if they are located in a specific country, as opposed to being stored in multiple locations or in places that offer better safeguards.

174. In addition, requiring Internet service providers to store data locally can create a barrier to entry into the market for new platforms and services. This would negatively affect the freedom of expression of users, who will see their access to resources for research, education, and communication reduced. Indeed, meeting the requirement of data localization is complex and costly, and harms individual users or new initiatives by potentially depriving them of the conditions of interoperability necessary to connect globally. Freedom of expression and democracy assume the free flow of information and require the prevention of measures that create fragmentation in the Internet."

iv. Transparency Requirements (extended)

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

"4. *Calls upon all States*... (*d*) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data..."

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1 (27 April 2016)

"43. The State party should increase the transparency of its surveillance policy."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/HRC/13/37 (28 December 2009)

"54. The application of secrecy privileges for surveillance systems inhibits the ability of legislatures, judicial bodies and the public to scrutinize State powers...

55. The principle of transparency and integrity requires openness and communication about surveillance practices...

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."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, U.N. Doc. A/HRC/23/40 (17 April 2013)

"91. States should be completely transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation and purpose.

92. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"39. A public legislative process provides an opportunity for Governments to justify mass surveillance measures to the public. Open debate enables the public to appreciate the balance that is being struck between privacy and security. A transparent law-making process should also identify the vulnerabilities inherent in digital communications systems, enabling users to make informed choices. This is not only a core ingredient of the requirement for legal certainty under article 17 of the Covenant; it is also a valuable means of ensuring effective public participation in a debate on a matter of national and international public interest...

40. By contrast, the use of delegated legislation (instruments enacted by the executive under delegated powers) has already permitted the adoption of secret legal frameworks for mass surveillance, inhibiting the ability of the legislature, the judiciary and the public to scrutinize the use of these new powers. Such provisions do not meet the quality of law requirements in article 17 of the Covenant because they are not sufficiently accessible to the public. While there may be legitimate public interest reasons for maintaining the secrecy of technical and operational specifications, these do not justify withholding from the public generic information about the nature and extent of a State's Internet penetration. Without such information, it is impossible to assess the legality, necessity and proportionality of these measures. States should therefore be transparent about the use and scope of mass communications surveillance (see A/HRC/23/40, para. 91)...

63. ...States should be transparent about the nature and extent of their Internet penetration, its methodology and its justification, and should provide a detailed public account of the tangible benefits that accrue from its use."

Parliamentary Assembly of the Council of Europe (PACE), Resolution on Mass Surveillance 2045 (21 April 2015)

"7. The Assembly unequivocally condemns the extensive use of secret laws and regulations, applied by secret courts using secret interpretations of the applicable rules, as this practice undermines public confidence in the judicial oversight mechanisms."

Escher et al. v. Brazil, Inter-American Court of Human Rights, Judgment (on Preliminary Objections, Merits, Reparations, and Costs), Series C No. 200, Concurring Opinion of Judge Sergio García Ramírez in relation to the Judgement (6 July 2009)

"6. We reject the furtiveness with which the tyrant hides his intolerable arbitrariness. We condemn the secrecy that shrouds the symbols of authoritarianism. We censure opacity in the exercise of public authority. We demand – and we are achieving, step by step, based on the

argument of human rights – transparency in the acts of Government and in the conduct of those who govern us…"

v. Safeguards in Intelligence Sharing and Data Transfers (extended)

Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, U.N. Doc CCPR/C/CAN/CO/6 (13 August 2015)

"10. Bill C-51 creates under the security of Canada Information Sharing Act, an increased sharing of information among federal government agencies on the basis of a very broad definition of activities that undermine the security of Canada which does not fully prevent that inaccurate or irrelevant information is shared... The State Party should... (c) Provide adequate safeguards to ensure that information-sharing under the Security of Canada Information Sharing Act does not result in human rights abuses..."

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (17 August 2015)

"24. The State Party should: ...(c) Ensure that robust oversight systems over surveillance, interception and intelligence-sharing of personal communications activities are in place, including by providing for judicial involvement in the authorization of such measures in all cases, and by considering the establishment of strong and independent oversight mandates with a view to preventing abuses."

Concluding Observations on the Initial Report of Pakistan, Human Rights Committee, U.N. Doc. CCPR/C/PAK/CO/1 (27 July 2017)

"35. While noting the State party's view that the Prevention of Electronic Crimes Act 2016 complies with the Convention on Cybercrime, the Committee is concerned that the Act provides for... (d) the sharing of information and cooperation with foreign governments without judicial authorization or oversight (arts. 17 and 19).

36. The State party should review its legislation on data collection and surveillance, in particular, the Prevention of Electronic Crimes Act 2016, to bring it in line with its obligations under the Covenant. It should … review its laws and practice of intelligence sharing with foreign agencies to ensure its compliance with the Covenant..."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/HRC/13/37 (28 December 2009)

"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... 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."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (17 April 2013)

"86. ...At the international level, States should enact Mutual Legal Assistance Treaties to regulate access to communications data held by foreign corporate actors."

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"30. The requirement of accessibility is also relevant when assessing the emerging practice of States to outsource surveillance tasks to others. There is credible information to suggest that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes. Such practice arguably fails the test of lawfulness because... it makes operation of the surveillance regime unforeseeable for those affected by it. It may undermine the essence of the right protected by Article 17 of the International Covenant on Civil and Political Rights... States have also failed to take effective measures to protect individuals within their jurisdiction against illegal surveillance practices by other States or business entities, in breach of their own human rights obligations."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"44. The absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority. Information concerning an individual's communications may be shared with foreign intelligence agencies without the protection of any publicly accessible legal framework and without adequate (or any) safeguards... Such practices make the operation of the surveillance regime unforeseeable for those affected by it and are therefore incompatible with article 17 of the Covenant."

U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017)

"...Expressing concern that individuals often do not provide their free, explicit and informed consent to the re-use, sale or multiple re-sales of their personal data, as the collecting, processing and sharing of personal data, including sensitive data, has increased significantly in the digital age..."

Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection, p. 11 (5 June 2015)

"The principle of making data available to other authorities should not be used to circumvent European and national constitutional data-protection standards."

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

"78. The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."

Parliamentary Assembly of the Council of Europe (PACE), Resolution on Mass Surveillance 2045 (21 April 2015)

"12. The Assembly also recognises the need for transatlantic co-operation in the fight against terrorism and other forms of organised crime. It considers that such co-operation must be based on mutual trust founded on international agreements, respect for human rights and the rule of law. This trust has been severely damaged by the mass surveillance practices revealed in the Snowden files.

13. In order to rebuild trust among the transatlantic partners, among the member States of the Council of Europe and also between citizens and their own governments, a legal framework must be put in place at the national and international levels which ensures the protection of human rights, especially the protection of the right to privacy. An effective tool for the enforcement of such a legal and technical framework, besides enhanced judicial and parliamentary scrutiny, is credible protection extended to whistle-blowers who expose violations...

19. The Assembly therefore urges the Council of Europe member and observer States to...

> 19.2. ensure, in order to enforce such a legal framework, that their intelligence services are subject to adequate judicial and/or parliamentary control mechanisms. Those responsible for national control mechanisms must have sufficient access to information and expertise and the power to review international co-operation without regard to the "originator control" principle, on a mutual basis...
>
> 19.4. agree on a multilateral "intelligence codex" for their intelligence services, which lays down rules governing co-operation for the purposes of the fight against terrorism and organised crime. The codex should include a mutual engagement to apply the same rules to the surveillance of partner states' nationals and residents as those applied to the surveillance of their own nationals and residents, and to share data obtained through lawful surveillance measures solely for the purposes for which they were collected. The use of surveillance measures for political, economic or diplomatic purposes in participating States should be banned."

European Commission For Democracy Through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006 (7 April 2015)

"11. Bulk transfers of data between States occur frequently. In order to avoid circumvention of rules on domestic intelligence gathering, it would be useful to provide that the bulk material transferred can only be searched if all the material requirements of a national search are fulfilled, and this is duly authorized in the same way as searches of bulk material obtained through national searches."

Maximillian Schrems v. Data Protection Commissioner (C-362/14), Court of Justice of the European Union, Grand Chamber, Judgment (6 October 2015)

"46. Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to the directive. In that regard, Chapter IV of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data...

63. Having regard to those considerations, where a person whose personal data has been or could be transferred to a third country which has been the subject of a Commission decision pursuant to Article 25(6) of Directive 95/46 lodges with a national supervisory authority a claim concerning the protection of his rights and freedoms in regard to the processing of that data and contests, in bringing the claim, as in the main proceedings, the compatibility of that decision with the protection of the privacy and of the fundamental rights and freedoms of individuals, it is incumbent upon the national supervisory authority to examine the claim with all due diligence...

70. It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection. In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country 'shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations' and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

71. However, first, as is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals'...

73. The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from the European Union to third countries for the purpose of being processed in those countries…

75. Accordingly, when examining the level of protection afforded by a third country, the Commission is obliged to assess the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country.

76. Also, in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted a decision pursuant to Article 25(6) of Directive 95/46, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard...

84. ...under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'...

87. In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States. To establish the existence of an interference with the fundamental right to respect for private life, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have suffered any adverse consequences on account of that interference...

90. ... the Commission found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

91. As regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court's settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data."

vi. Distinctions in Safeguards Between Metadata and Content and Between GEOINT and SIGINT (extended)

U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017)

"...Noting also that, while metadata may provide benefits, certain types of metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications and can give an insight into an individual's behaviour, social relationships, private preferences and identity..."

Uzun v. Germany, App. No. 35623/05, European Court of Human Rights, Judgment (2 September 2010)

"44. There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person walking along the street will inevitably be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain.

45. Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that normally foreseeable.

46. Thus, the Court has considered that the systematic collection and storing of data by security services on particular individuals, even without the use of covert surveillance methods, constituted an interference with these persons' private lives...

47. The Court has further taken into consideration whether the impugned measure amounted to a processing or use of personal data of a nature to constitute an interference with respect for private life. Thus, it considered, for instance, the permanent recording of footage deliberately taken of the applicant at a police station by a security camera and its use in a video identification procedure as the processing of personal data about the applicant interfering with his right to respect for private life. Likewise, the covert and permanent recording of the applicants' voices at a police station for further analysis as voice samples directly relevant for identifying these persons in the context of other personal data was regarded as the processing of personal data about them amounting to an interference with their private lives...

51. ... by the surveillance of the applicant via GPS, the investigation authorities, for some three months, systematically collected and stored data determining, in the circumstances, the applicant's whereabouts and movements in the public sphere. They further recorded the personal data and used it in order to draw up a pattern of the applicant's movements, to make further investigations and to collect additional evidence at the places the applicant had travelled to, which was later used at the criminal trial against the applicant.

52. In the Court's view, GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings. Having regard to the principles established in its case-law, it nevertheless finds the above-mentioned factors sufficient to conclude that the applicant's observation via GPS, in the circumstances, and the processing and use of the data obtained thereby in the manner described above amounted to an interference with his private life as protected by Article 8 § 1...

66. While the Court is not barred from gaining inspiration from [the Weber principles], it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications, are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations. It will therefore apply the more general principles on adequate protection against arbitrary interference with Article 8 rights as summarised above...

69. In examining whether domestic law contained adequate and effective guarantees against abuse, the Court observes that in its nature conducting surveillance of a person by building a GPS receiver into the car he or she uses, coupled with visual surveillance of that person, permits the authorities to track that person's movements in public places whenever he or she is travelling in that car. It is true that, as the applicant had objected, there was no fixed statutory limit on the duration of such monitoring. A fixed time- limit had only subsequently been enacted in so far as under the new Article163f § 4 of the Code of Criminal Procedure, the systematic surveillance of a suspect ordered by a Public Prosecutor could not exceed one month, and any further extension could only be ordered by a judge. However, the Court is satisfied that the duration of such a surveillance measure was subject to its proportionality in the circumstances and that the domestic courts reviewed the respect of the proportionality principle in this respect. It finds that German law therefore provided sufficient guarantees against abuse on that account."

Shimovolos v. Russia, App. No. 30194/09, European Court of Human Rights, Judgment (21 June 2011)

"64. The Court reiterates that private life is a broad term not susceptible to exhaustive definition. Article 8 is not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world. Private life may even include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".

65. The Court has earlier found that the systematic collection and storing of data by security services on particular individuals constituted an interference with these persons' private lives, even if that data was collected in a public place or concerned exclusively the person's professional or public activities. Collection, through a GPS device attached to a person's car, and storage of data concerning that person's whereabouts and movements in the public sphere was also found to constitute an interference with private life.

66. Turning to the circumstances of the present case, the Court observes that the applicant's name was registered in the Surveillance Database which collected information about his movements, by train or air, within Russia. Having regard to its case-law cited in paragraphs 64 and 65 above, the Court finds that the collection and storing of that data amounted to an interference with his private life as protected by Article 8 § 1 of the Convention."

Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)

"26. …it should be observed that the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

27. Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.

28. In such circumstances, even though, as is apparent from Article 1(2) and Article 5(2) of Directive 2006/24, the directive does not permit the retention of the content of the communication or of information consulted using an electronic communications network, it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter.

29. The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such a retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data within the meaning of that article and, therefore, necessarily has to satisfy the data protection requirements arising from that article."

Draft agreement between Canada and the European Union on the Transfer of Passenger Name Record data (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)

"121. As set out in the Annex to the envisaged agreement, the PNR data covered by that agreement includes, inter alia, and besides the name(s) of the air passenger(s), information

necessary to the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation number, passenger contact information, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers...

122. Since the PNR data therefore includes information on identified individuals, namely air passengers flying between the European Union and Canada, the various forms of processing to which, under the envisaged agreement, that data may be subject, namely its transfer from the European Union to Canada, access to that data with a view to its use or indeed its retention, affect the fundamental right to respect for private life..."

vii. Distinctions in Safeguards Between Law Enforcement and Intelligence Agencies (extended)

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, U.N. Doc. CCPR/C/POL/CO/7 (4 November 2016)

"39. The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities as reflected in the Law on Counterterrorism of June 2016 and the Act amending the Police Act and certain other acts of January 2016. The Committee is particularly concerned about: a) the unlimited and indiscriminate surveillance of communications and collection of metadata..."

viii. Professional Confidentiality and Privileged Communications (extended)

Iordachi and Others v. Moldova, App. No. 25198/02, European Court of Human Rights, Judgment (24 September 2009)

"50. As regards the interception of communications of persons suspected of offences, the Court observes that in Kopp it found a violation of Article 8 because the person empowered under Swiss secret surveillance law to draw a distinction between matters connected with a lawyer's work and other matters was an official of the Post Office's legal department. In the present case, while the Moldovan legislation, like the Swiss legislation, guarantees the secrecy of lawyer-client communications, it does not provide for any procedure which would give substance to the above provision. The Court is struck by the absence of clear rules defining what should happen when, for example, a phone call made by a client to his lawyer is intercepted.

Parliamentary Assembly of the Council of Europe (PACE), Resolution on Mass Surveillance 2045 (21 April 2015)

"4. The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 of the European Convention on Human Rights (ETS No. 5)), freedom of information and expression (Article 10), a fair trial (Article 6) and freedom of religion (Article 9) – especially when confidential communications with lawyers and religious ministers are intercepted and when digital evidence is manipulated. These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardises the rule of law..."

Tristán Donoso v. Panamá, Inter-American Court of Human Rights, Judgment (on Preliminary Objection, Merits, Reparations, and Costs), Series C No. 193 (27 January 2009)

"75. The Court considers the telephone conversation between Mr. Zayed and Mr. Tristán Donoso to have been private and that none of the two of them consented to its disclosure to third parties. Moreover, as such conversation was held between the alleged victim [A Lawyer] and one of his clients, it should even be afforded a greater degree of protection on account of professional secrecy.'"

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

158. ...The ideological basis of all these regimes was the 'National Security Doctrine,' which regarded leftist movements and other groups as 'common enemies'." Even today, it has been reported that national security reasons tend to be invoked to place human rights defenders, journalists, members of the media, and activists under surveillance, or to justify excessive secrecy in the decision-making processes and investigations tied to surveillance issues. Clearly, this kind of interpretation of the "national security" objective cannot be the basis for the establishment of surveillance programs of any kind, including, naturally, online communications surveillance programs."

E. The Principle of Access to Remedy: Victimhood, Standing, and Notification (extended)

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

"4. *Calls upon all States*... (*e*) To provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations..."

U.N. Human Rights, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (8 April 1988)

"10. ... In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files."

Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, Human Rights Committee, U.N. Doc. CCPR/C/MKD/CO/3 (17 August 2015)

"23. ...[The State Party should] ensure that persons who are unlawfully monitored are systematically informed thereof and have access to adequate remedies."

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (17 August 2015)

"24. The State Party Should: ...(e) Ensure that persons affected have access to effective remedies in cases of abuse."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"61. ...States should not impose standing requirements that undermine the right to an effective remedy."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (17 April 2013)

"82. Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath."

Klass and Others v. Germany, App. No. 5029/71, European Court of Human Rights, Judgment (6 September 1978)

"34. ...the question arises in the present proceedings whether an individual is to be deprived of the opportunity of lodging an application with the Commission because, owing to the secrecy of the measures objected to, he cannot point to any concrete measure specifically affecting him. In the Court's view, the effectiveness (l'effet utile) of the Convention implies in such circumstances some possibility of having access to the Commission. If this were not so, the efficiency of the Convention's enforcement machinery would be materially weakened. The procedural provisions of the Convention must, in view of the fact that the Convention and its institutions were set up to protect the individual, be applied in a manner which serves to make the system of individual applications efficacious. The Court therefore accepts that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures...

36. The Court points out that where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8, or even to be deprived of the right granted by that Article, without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions... The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by

the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation. A right of recourse to the Commission for persons potentially affected by secret surveillance is to be derived from Article 25, since otherwise Article 8 runs the risk of being nullified.

37. As to the facts of the particular case, the Court observes that the contested legislation institutes a system of surveillance under which all persons in the Federal Republic of Germany can potentially have their mail, post and telecommunications monitored, without their ever knowing this unless there has been either some indiscretion or subsequent notification in the circumstances laid down in the Federal Constitutional Court's judgment. To that extent, the disputed legislation directly affects all users or potential users of the postal and telecommunication services in the Federal Republic of Germany. Furthermore, as the Delegates rightly pointed out, this menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8 (art. 8). At the hearing, the Agent of the Government informed the Court that at no time had surveillance measures under the G 10 been ordered or implemented in respect of the applicants. The Court takes note of the Agent's statement. However, in the light of its conclusions as to the effect of the contested legislation the Court does not consider that this retrospective clarification bears on the appreciation of the applicants' status as "victims".

38. Having regard to the specific circumstances of the present case, the Court concludes that each of the applicants is entitled to "(claim) to be the victim of a violation" of the Convention, even though he is not able to allege in support of his application that he has been subject to a concrete measure of surveillance. The question whether the applicants were actually the victims of any violation of the Convention involves determining whether the contested legislation is in itself compatible with the Convention's provisions. Accordingly, the Court does not find it necessary to decide whether the Convention implies a right to be informed in the circumstances mentioned by the Principal Delegate.

41. ... Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8, the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision... Neither before the Commission nor before the Court did the Government contest this issue. Clearly, any of the permitted surveillance measures, once applied to a given individual, would result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence. Furthermore, in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence. The Court does not exclude that the contested legislation, and therefore the measures permitted thereunder, could also involve an interference with the exercise of a person's right to respect for his home. However, the Court does not deem it necessary in the present proceedings to decide this point…

57. As regards review a posteriori, it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual

concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality. The applicants' main complaint under Article 8 (art. 8) is in fact that the person concerned is not always subsequently informed after the suspension of surveillance and is not therefore in a position to seek an effective remedy before the courts. Their preoccupation is the danger of measures being improperly implemented without the individual knowing or being able to verify the extent to which his rights have been interfered with. In their view, effective control by the courts after the suspension of surveillance measures is necessary in a democratic society to ensure against abuses; otherwise adequate control of secret surveillance is lacking and the right conferred on individuals under Article 8 (art. 8) is simply eliminated. In the Government's view, the subsequent notification which must be given since the Federal Constitutional Court's judgment corresponds to the requirements of Article 8 para. 2 (art. 8-2). In their submission, the whole efficacy of secret surveillance requires that, both before and after the event, information cannot be divulged if thereby the purpose of the investigation is, or would be retrospectively, thwarted. They stressed that recourse to the courts is no longer excluded after notification has been given, various legal remedies then becoming available to allow the individual, inter alia, to seek redress for any injury suffered.

58. In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the "interference" resulting from the contested legislation is in principle justified under Article 8 para. 2 (art. 8-2), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the "interference". Moreover, it is to be recalled that, in pursuance of the Federal Constitutional Court's judgment of 15 December 1970, the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardising the purpose of the restriction."

Malone v. The United Kingdom, App. No. 8691/79, European Court of Human Rights, Judgment (2 August 1984)

"64. Despite the applicant's allegations, the Government have consistently declined to disclose to what extent, if at all, his telephone calls and mail have been intercepted otherwise on behalf of the police...

86. The applicant, as a suspected receiver of stolen goods, was, it may be presumed, a member of a class of persons potentially liable to be directly affected by this practice. The applicant can therefore claim, for the purposes of Article 25 (art. 25) of the Convention, to be a "victim" of a violation of Article 8 (art. 8) by reason of the very existence of this practice, quite apart from any concrete measure of implementation taken against. This remains so despite the clarification by the Government that in fact the police had neither caused his telephone to be metered nor undertaken any search operations on the basis of any list of telephone numbers obtained from metering."

Rotaru v. Romania, App. No. 28341/95, European Court of Human Rights, Judgment (4 May 2000)

"35. The Court reiterates, as to the concept of victim, that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. Furthermore, "a decision or measure favourable to the applicant is not in principle sufficient to deprive him of his status as a 'victim' unless the national authorities have acknowledged, either expressly or in substance, and then afforded redress for, the breach of the Convention".

36. In the instant case the Court notes that the applicant complained of the holding of a secret register containing information about him, whose existence was publicly revealed during judicial proceedings. It considers that he may on that account claim to be the victim of a violation of the Convention... Assuming that it may be considered that [the 25 November 1997 judgment of the Bucharest Court of Appeal] did, to some extent, afford the applicant redress for the existence in his file of information that proved false, the Court takes the view that such redress is only partial and that at all events it is insufficient under the case-law to deprive him of his status of victim..."

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

"78. The Court further notes that the applicants, even though they were members of a group of persons who were likely to be affected by measures of interception, were unable to demonstrate that the impugned measures had actually been applied to them. It reiterates, however, its findings in comparable cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them...

135. The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively. However, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democracy society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. Indeed, such notification might reveal the working methods and fields of operation of the Intelligence Service. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned."

Liberty and Others v. The United Kingdom, App. No. 58243/00, European Court of Human Rights, Judgment (1 July 2008)

"56. Telephone, facsimile and e-mail communications are covered by the notions of "private life" and "correspondence" within the meaning of Article 8. The Court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.

57. The Court notes that the Government are prepared to proceed, for the purposes of the present application, on the basis that the applicants can claim to be victims of an interference with their communications sent to or from their offices in the United Kingdom and Ireland. In any event, under Section 3(2) the 1985 Act, the authorities were authorised to capture communications contained within the scope of a warrant issued by the Secretary of State and to listen to and examine communications falling within the terms of a certificate, also issued by the Secretary of State. Under section 6 of the 1985 Act arrangements had to be made regulating the disclosure, copying and storage of intercepted material. The Court considers that the existence of these powers, particularly those permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants, since they were persons to whom these powers might have been applied."

Iordachi and Others v. Moldova, App. No. 25198/02, European Court of Human Rights, Judgment (24 September 2009)

"31. The Court notes that under the Operational Investigative Activities Act the authorities are authorised to intercept communications of certain categories of persons provided for in section 6 of that Act. In their capacity as human rights lawyers the applicants represent and thus have extensive contact with such persons...

33. ...the Court considers that it cannot be excluded that secret surveillance measures were applied to the applicants or that they were at the material time potentially at risk of being subjected to such measures.

34. The mere existence of the legislation entails, for all those who might fall within its reach, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunications services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for correspondence."

Kennedy v. The United Kingdom, App. No. 26839/05, European Court of Human Rights, Judgment (18 May 2010)

"126. The applicant has alleged that the fact that calls were not put through to him and that he received hoax calls demonstrates a reasonable likelihood that his communications are being intercepted. The Court disagrees that such allegations are sufficient to support the applicant's contention that his communications have been intercepted. Accordingly, it concludes that the applicant has failed to demonstrate a reasonable likelihood that there was actual interception in his case.

127. Insofar as the applicant complains about the RIPA regime itself, the Court observes, first, that the RIPA provisions allow any individual who alleges interception of his communications to lodge a complaint with an independent tribunal, a possibility which was taken up by the applicant. The IPT concluded that no unlawful, within the meaning of RIPA, interception had taken place.

128. As to whether a particular risk of surveillance arises in the applicant's case, the Court notes that under the provisions of RIPA on internal communications, any person within the United Kingdom may have his communications intercepted if interception is deemed necessary on one or more of the grounds listed in section 5(3). The applicant has alleged that he is at particular risk of having his communications intercepted as a result of his high-profile murder case, in which he made allegations of police impropriety, and his subsequent campaigning against miscarriages of justice. The Court observes that neither of these reasons would appear to fall within the grounds listed in section 5(3) RIPA. However, in light of the applicant's allegations that any interception is taking place without lawful basis in order to intimidate him, the Court considers that it cannot be excluded that secret surveillance measures were applied to him or that he was, at the material time, potentially at risk of being subjected to such measures."

Dragojević v. Croatia, App. No. 68955/11, European Court of Human Rights, Judgment (15 January 2015)

"99. [There is no adequate and sufficient safeguards against abuse] in cases where the only effective possibility for an individual subjected to covert surveillance in the context of criminal proceedings is to challenge the lawfulness of the use of such measures before the criminal courts during the criminal proceedings against him or her. The Court has already held that although the courts could, in the criminal proceedings, consider questions of the fairness of admitting the evidence in the criminal proceedings, it was not open to them to deal with the substance of the Convention complaint that the interference with the applicant's right to respect for his private life was not "in accordance with the law"; still less was it open to them to grant appropriate relief in connection with the complaint.

100. This can accordingly be observed in the present case, where the competent criminal courts limited their assessment of the use of secret surveillance to the extent relevant to the admissibility of the evidence thus obtained, without going into the substance of the Convention requirements concerning the allegations of arbitrary interference with the applicant's Article 8 rights. At the same time, the Government have not provided any information on remedies – such as an application for a declaratory judgment or an action for damages – which may become available to a person in the applicant's situation."

Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015)

"164. The Court has consistently held in its case-law that the Convention does not provide for the institution of an actio popularis and that its task is not normally to review the relevant law and practice in abstracto, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention. Accordingly, in order to be able to lodge an application in accordance with Article 34, an individual must be able to show that he or she was "directly affected" by the measure complained of. This is indispensable for putting the protection mechanism of the Convention into motion, although this criterion is not to be applied in a rigid, mechanical and inflexible way throughout the proceedings.

165. Thus, the Court has permitted general challenges to the relevant legislative regime in the sphere of secret surveillance in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them. In the case of Klass and Others v. Germany the Court held that an individual might, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures had been in fact applied to him. The relevant conditions were to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures...

166. Following the Klass and Others case, the case-law of the Convention organs developed two parallel approaches to victim status in secret surveillance cases.

167. In several cases the Commission and the Court held that the test in Klass and Others could not be interpreted so broadly as to encompass every person in the respondent State who feared that the security services might have compiled information about him or her. An applicant could not, however, be reasonably expected to prove that information concerning his or her private life had been compiled and retained. It was sufficient, in the area of secret measures, that the existence of practices permitting secret surveillance be established and that there was a reasonable likelihood that the security services had compiled and retained information concerning his or her private life...

168. In other cases the Court reiterated the Klass and Others approach that the mere existence of laws and practices which permitted and established a system for effecting secret surveillance of communications entailed a threat of surveillance for all those to whom the legislation might be applied. This threat necessarily affected freedom of communication between users of the telecommunications services and thereby amounted in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them...

169. Finally, in its most recent case on the subject, Kennedy v. the United Kingdom, the Court held that sight should not be lost of the special reasons justifying the Court's departure, in cases concerning secret measures, from its general approach which denies individuals the right to challenge a law in abstracto. The principal reason was to ensure that the secrecy of such measures did not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and the Court. In order to assess, in a particular case, whether an individual can claim an interference as a result of the mere existence of legislation permitting secret surveillance measures, the Court must have regard to the availability of any remedies at the national level and the risk of secret surveillance measures being applied to him or her. Where there is no possibility of challenging the alleged application of secret surveillance measures at domestic level, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court.

170. The Court considers, against this background, that it is necessary to clarify the conditions under which an applicant can claim to be the victim of a violation of Article 8 without having

to prove that secret surveillance measures had in fact been applied to him, so that a uniform and foreseeable approach may be adopted.

171. In the Court's view the Kennedy approach is best tailored to the need to ensure that the secrecy of surveillance measures does not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and of the Court. Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. As the Court underlined in Kennedy, where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law in abstracto, is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures.

172. The Kennedy approach therefore provides the Court with the requisite degree of flexibility to deal with a variety of situations which might arise in the context of secret surveillance, taking into account the particularities of the legal systems in the member States, namely the available remedies, as well as the different personal situations of applicants...

175. The Court notes that the contested legislation institutes a system of secret surveillance under which any person using mobile telephone services of Russian providers can have his or her mobile telephone communications intercepted, without ever being notified of the surveillance. To that extent, the legislation in question directly affects all users of these mobile telephone services.

176. Furthermore, for the reasons set out below, Russian law does not provide for effective remedies for a person who suspects that he or she was subjected to secret surveillance.

177. In view of the above finding, the applicant does not need to demonstrate that, due to his personal situation, he is at risk of being subjected to secret surveillance.

178. Having regard to the secret nature of the surveillance measures provided for by the contested legislation, the broad scope of their application, affecting all users of mobile

telephone communications, and the lack of effective means to challenge the alleged application of secret surveillance measures at domestic level, the Court considers an examination of the relevant legislation in abstracto to be justified.

179. The Court therefore finds that the applicant is entitled to claim to be the victim of a violation of the Convention, even though he is unable to allege that he has been subject to a concrete measure of surveillance in support of his application. For the same reasons, the mere existence of the contested legislation amounts in itself to an interference with the exercise of his rights under Article 8. The Court therefore dismisses the Government's objection concerning the applicant's lack of victim status...

286. The Court will now turn to the issue of notification of interception of communications which is inextricably linked to the effectiveness of remedies before the courts.

287. It may not be feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned. The Court also takes note of the Recommendation of the Committee of Ministers regulating the use of personal data in the police sector, which provides that where data concerning an individual have been collected and stored without his or her knowledge, and unless the data are deleted, he or she should be informed, where practicable, that information is held about him or her as soon as the object of the police activities is no longer likely to be prejudiced.

288. In the cases of Klass and Others and Weber and Saravia the Court examined German legislation which provided for notification of surveillance as soon as that could be done after its termination without jeopardising its purpose. The Court took into account that it was an independent authority, the G10 Commission, which had the power to decide whether an individual being monitored was to be notified of a surveillance measure. The Court found that the provision in question ensured an effective notification mechanism which contributed to keeping the interference with the secrecy of telecommunications within the limits of what was necessary to achieve the legitimate aims pursued. In the cases of Association for European Integration and Human Rights and Ekimdzhiev and Dumitru Popescu (no. 2), the Court found that the absence of a requirement to notify the subject of interception at any point was incompatible with the Convention, in that it deprived the interception subject of an opportunity to seek redress for unlawful interferences with his or her Article 8 rights and rendered the remedies available under the national law theoretical and illusory rather than practical and effective. The national law thus eschewed an important safeguard against the improper use of special means of surveillance. By contrast, in the case of Kennedy the absence of a requirement to notify the subject of interception at any point in time was compatible with the Convention, because in the United Kingdom any person who suspected that his communications were being

or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception subject that there had been an interception of his or her communications.

289. Turning now to the circumstances of the present case, the Court observes that in Russia persons whose communications have been intercepted are not notified of this fact at any point or under any circumstances. It follows that, unless criminal proceedings have been opened against the interception subject and the intercepted data have been used in evidence, or unless there has been a leak, the person concerned is unlikely ever to find out if his or her communications have been intercepted.

290. The Court takes note of the fact that a person who has somehow learned that his or her communications have been intercepted may request information about the corresponding data. It is worth noting in this connection that in order to be entitled to lodge such a request the person must be in possession of the facts of the operational search measures to which he or she was subjected. It follows that the access to information is conditional on the person's ability to prove that his or her communications were intercepted. Furthermore, the interception subject is not entitled to obtain access to documents relating to interception of his or her communications; he or she is at best entitled to receive "information" about the collected data. Such information is provided only in very limited circumstances, namely if the person's guilt has not been proved in accordance with the procedure prescribed by law, that is, he or she has not been charged or the charges have been dropped on the ground that the alleged offence was not committed or that one or more elements of a criminal offence were missing. It is also significant that only information that does not contain State secrets may be disclosed to the interception subject and that under Russian law information about the facilities used in operational search activities, the methods employed, the officials involved and the data collected constitutes a State secret. In view of the above features of Russian law, the possibility to obtain information about interceptions appears to be ineffective.

291. The Court will bear the above factors – the absence of notification and the lack of an effective possibility to request and obtain information about interceptions from the authorities – in mind when assessing the effectiveness of remedies available under Russian law.

292. Russian law provides that a person claiming that his or her rights have been or are being violated by a State official performing operational search activities may complain to the official's superior, a prosecutor or a court. The Court reiterates that a hierarchical appeal to a direct supervisor of the authority whose actions are being challenged does not meet the requisite standards of independence needed to constitute sufficient protection against the abuse of authority. A prosecutor also lacks independence and has a limited scope of review, as demonstrated above. It remains to be ascertained whether a complaint to a court may be regarded as an effective remedy...

294. ...Given that the Government did not submit any examples of domestic practice on examination of cassation appeals, the Court has strong doubts as to the existence of a right to lodge a cassation appeal against a judicial decision authorising interception of communications. At the same time, the interception subject is clearly entitled to lodge a supervisory review complaint however, in order to lodge a supervisory review complaint against the judicial decision authorising interception of communications, the person concerned must be aware that such a decision exists. Although the Constitutional Court has held that it is not necessary to attach a copy of the contested judicial decision to the supervisory review complaint, it is

difficult to imagine how a person can lodge such a complaint without having at least the minimum information about the decision he or she is challenging, such as its date and the court which has issued it. In the absence of notification of surveillance measures under Russian law, an individual would hardly ever be able to obtain that information unless it were to be disclosed in the context of criminal proceedings against him or her or there was some indiscretion which resulted in disclosure...

298. The Court concludes from the above that the remedies referred to by the Government are available only to persons who are in possession of information about the interception of their communications. Their effectiveness is therefore undermined by the absence of a requirement to notify the subject of interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities. Accordingly, the Court finds that Russian law does not provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject. It is not the Court's task in the present case to decide whether these remedies will be effective in cases where an individual learns about the interception of his or her communications in the course of criminal proceedings against him or her...

300. In view of the above considerations, the Court finds that Russian law does not provide for effective remedies to a person who suspects that he or she has been subjected to secret surveillance. By depriving the subject of interception of the effective possibility of challenging interceptions retrospectively, Russian law thus eschews an important safeguard against the improper use of secret surveillance measures."

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

"33. ...in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has accepted that, under certain circumstances, an individual may claim to be a victim on account of the mere existence of legislation permitting secret surveillance, even if he cannot point to any concrete measures specifically affecting him.

36. ... Most recently, the Court adopted, in Roman Zakharov v. Russia, a harmonised approach based on Kennedy, according to which firstly the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affect all users of communication services by instituting a system where any person can have his or her communications intercepted; and secondly the Court will take into account the availability or remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies.

37. The Court observes that the present applicants complained of an interference with their homes, communications and privacy on the basis of the very existence of the law permitting secret surveillance and the lack of adequate safeguards, admitting that their personal or professional situations were not of the kind that might normally attract the application of surveillance measures. They nevertheless thought they were at particular risk of having their communications intercepted as a result of their employment with civil-society organisations criticising the Government.

38. The Court observes that affiliation with a civil-society organisation does not fall within the grounds listed in section 7/E (1) point (a) sub-point (ad) and point (e) of the Police Act, which concern in essence terrorist threats and rescue operations to the benefit of Hungarian citizens in dangerous situations abroad. Nevertheless, it appears that under these provisions any person within Hungary may have his communications intercepted if interception is deemed necessary on one of the grounds enumerated in the law. The Court considers that it cannot be excluded that the applicants are at risk of being subjected to such measures should the authorities perceive that to do so might be of use to pre-empt or avert a threat foreseen by the legislation – especially since the law contains the notion of "persons concerned identified ... as a range of persons" which might include indeed any person. The Court also notes that, by examining their constitutional complaint on the merits, the Constitutional Court implicitly acknowledged the applicants' being personally affected by the legislation in question for the purposes of section 26(1) of the Act on the Constitutional Court. It is of importance at this juncture to note that they are staff members of a watchdog organisation, whose activities have previously been found similar, in some ways, to those of journalists. The Court accepts the applicants' suggestion that any fear of being subjected to secret surveillance might have an impact on such activities. In any case, whether or not the applicants belong to a targeted group, the Court considers that the legislation directly affects all users of communication systems and all homes.

39. Considering in addition that the domestic law does not appear to provide any possibility for an individual who alleges interception of his or her communications to lodge a complaint with an independent body, the Court is of the view that the applicants can claim to be victims of a violation of their rights under the Convention, within the meaning of Article 34 of the Convention...

86. Moreover, the Court has held that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned. In Hungarian law, however, no notification, of any kind, of the measures is foreseen. This fact, coupled with the absence of any formal remedies in case of abuse, indicates that the legislation falls short of securing adequate safeguards.

87. It should be added that although the Constitutional Court held that various provisions in the domestic law read in conjunction secured sufficient safeguards for data storage, processing and deletion, special reference was made to the importance of individual complaints made in this context. For the Court, the latter procedure is hardly conceivable, since once more it transpires from the legislation that the persons concerned will not be notified of the application of secret surveillance to them."

Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016)

"121. ...the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that

notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed."

Draft agreement between Canada and the European Union on the Transfer of Passenger Name Record data (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)

"224. ...information must, in accordance with the case-law [...], be provided only once it is no longer liable to jeopardise the investigations being carried out by the government authorities referred to in the envisaged agreement.

225. The envisaged agreement should therefore specify that air passengers whose PNR data has been used and retained by the Canadian Competent Authority [...] and those whose data has been disclosed to other government authorities or to individuals, are to be notified, by that authority, of such use and such disclosure...

226. As regards air passengers' right to redress, Article 14(2) of the envisaged agreement provides that Canada is to ensure that any individual who is of the view that their rights have been infringed by a decision or action in relation to their PNR data may seek effective judicial redress, in accordance with Canadian law, or such other remedy which may include compensation.

227. Since that provision refers to 'any individual who is of the view that their rights have been infringed', it covers all air passengers, regardless of their nationality, their residence, their domicile or their presence in Canada. Furthermore, it must, as the Council has observed, be understood as meaning that air passengers have a legal remedy before a tribunal..."

Chapter 3B: Surveillance and Other Human Rights Provisions

A. Surveillance and the Jurisdictional Clause (Extraterritorial Application) (extended)

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 August 2015); Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4, para. 22 (23 April 2014)

"measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance".

Concluding Observations on the Sixth Periodic Report of New Zealand, Human Rights Committee, U.N. Doc. CCPR/C/NZL/CO/6 (28 April 2016)

"15. The Committee is further concerned about the limited judicial authorization process for the interception of communications of New Zealanders and the total absence of such authorization for the interception of communications of non-New Zealanders.

16. The State party should take all appropriate measures to ensure that: ...(b) Sufficient judicial safeguards are implemented, regardless of the nationality or location of affected persons, in terms of interception of communications and metadata collection, processing and sharing."

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, U.N. Doc. CCPR/C/POL/CO/7 (4 November 2016)

"39. The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities as reflected in the Law on Counterterrorism of June 2016 and the Act amending the Police Act and certain other acts of January 2016. The Committee is particularly concerned about: ...(b) the targeting of foreign nationals and application of different legal criteria to them."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"62. The Special Rapporteur concurs with the High Commissioner for Human rights that where States penetrate infrastructure located outside their territorial jurisdiction, they remain bound by their obligations under the Covenant."

John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, Brief of Amici Curiae, United Nations Human Rights Experts in Support of Plaintiff-Appellant and Reversal, D.C. Ct. App., Case No. 16-7081, pp. 6-7, 21 (1 November 2016)

"...[A]ll States Parties to the Covenant under Article 2(1), "[u]ndertake[] to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized

in the present Covenant." This undertaking "implies an affirmative obligation by the state to take whatever measures are necessary to enable individuals to enjoy or exercise [these rights] ... including the removal of governmental and possibly also some private obstacles to the enjoyment of these rights."...

In most situations, the United States may be able to meet these obligations through the application of Constitutional and statutory law at the federal, state, and local levels of government, whether through judicial, legislative or administrative means. Human rights law requires that governments "ensure" protection of individuals' rights not only against the State but also third parties. In a case like the instant one, in which the Government responsibility involves its citizen's rights within its territory against a third party State, the availability of specific legal frameworks, such as the [Foreign Sovereign Immunities Act], enables the United States to meet its Article 2 obligations…

Ethiopia's alleged surveillance of Kidane does not merely violate the rights guaranteed under the Covenant. State practice and the jurisprudence of international regional human rights bodies establish global consensus that digital surveillance measures intended to disrupt or deter the work of human rights defenders and activists violate well-established human rights norms. Recognizing that U.S. law provides a vehicle to redress these violations would align the United States with the international community and send a strong global signal against such digital attacks."

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

87. The Court reiterates that the term "law" within the meaning of the Convention refers back to national law, including rules of public international law applicable in the State concerned. As regards allegations that a respondent State has violated international law by breaching the territorial sovereignty of a foreign State, the Court requires proof in the form of concordant inferences that the authorities of the respondent State have acted extraterritorially in a manner that is inconsistent with the sovereignty of the foreign State and therefore contrary to international law.

88. The Court observes that the impugned provisions of the amended G10 Act authorise the monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and the use of data thus obtained. Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States are protected in public intentional law."

European Commission For Democracy Through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006 (7 April 2015)

"6. The collection of signals intelligence may legitimately take place on the territory of another state with its consent, but might still fall under the jurisdiction of the collecting state from the

view point of human rights obligations under the ECHR. At any rate, the processing, analysis and communication of this material clearly falls under the jurisdiction of the collecting State and is governed by both national law and the applicable human rights standards. There may be competition or even incompatibility between obligations imposed on telecommunications companies by the collecting state and data protection obligations in the territorial state; minimum international standards on privacy protection appear all the more necessary."

B. Surveillance and the Principle of Non-Discrimination (extended)

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, U.N. Doc. CCPR/C/POL/CO/7 (4 November 2016)

"39. The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities as reflected in the Law on Counterterrorism of June 2016 and the Act amending the Police Act and certain other acts of January 2016. The Committee is particularly concerned about: ...(b) the targeting of foreign nationals and application of different legal criteria to them."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"62. …Moreover, article 26 of the Covenant prohibits discrimination on grounds of, inter alia, nationality and citizenship. The Special Rapporteur thus considers that States are legally obliged to afford the same privacy protection for nationals and non-nationals and for those within and outside their jurisdiction. Asymmetrical privacy protection regimes are a clear violation of the requirements of the Covenant."

Report of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/71368 (30 August 2016)

"36. ...what is the true value of laws that discriminate between nationals and non-nationals? Especially since, in terms of article 17 of the International Covenant on Civil and Political Rights, everybody enjoys a right to privacy irrespective of nationality or citizenship, so one must ask how useful and appropriate, never mind legal, such types of provisions may be... This interpretation is as unacceptable as any claim in the laws of other countries that fundamental human rights protection is only restricted to its own citizens or residents."

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/HRC/34/61 (21 February 2017)

"33. ...[there are] serious and continuing concerns around extraterritorial mass surveillance programmes, and proliferation of laws that authorize asymmetrical protection regimes for nationals and non-nationals. Such laws exist in Germany, France, and the United States. The Special Rapporteur recalls that differential treatment of nationals and non-nationals, and of those within or outside a State's jurisdiction, is incompatible with the principle of non-discrimination, which is a key constituent of any proportionality assessment."

U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017)

"...Noting with concern that automatic processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights, and recognizing the need to further discuss and analyse these practices on the basis of international human rights law..."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"163. When establishing [any limitations on the right to privacy], States must abstain from perpetuating prejudice and discrimination. Accordingly, limitations to the exercise of fundamental rights cannot be discriminatory or have discriminatory effects, as this would also be inconsistent with Articles 1.1 and 24 of the American Convention. It bears recalling that, under Article 13 of the American Convention, freedom of expression is a right that belongs to "everyone," and by virtue of Principle 2 of the Declaration of Principles, "[a]ll people should be afforded equal opportunities to receive, seek and impart information by any means of communication without any discrimination for reasons of race, color, sex, language, religion, political or other opinions, national or social origin, economic status, birth or any other social condition."

Chapter 4B: Mass Surveillance Programs

Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Request for the Indication of Provisional Measures, Separate Opinion of Judge Cançado Trindade I.C.J. Reports 2014, p. 167 (3 March 2014).

"51. Six and a half decades ago (in 1949), in his last book, Nineteen Eighty-Four, George Orwell repeatedly warned: "Big Brother Is Watching You". Modern history is permeated with examples of the undue exercise of search and seizure, by those who felt powerful enough to exercise unreasonable surveillance of others. Modern history has also plenty of examples of the proper reaction of those who felt victimized by such exercise of search and seizure. In so reacting, the latter felt that, though lacking in factual power, they had law on their side, as all are equal before the law. If Orwell could rise from his tomb today, I imagine he would probably contemplate writing Two Thousand Eighty-Four, updating his perennial and topical warning, so as to encompass surveillance not only at intra-State level, but also at inter-State level; nowadays, "Big Brother Is Watching You" on a much wider geographical scale, and also in the relations across nations."

Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, U.N. Doc CCPR/C/CAN/CO/6 (13 August 2015)

"10. [T]he Committee is concerned about information according to which (a) Bill C-51 amendments to the Canadian Security Intelligence Act confers a broad mandate and powers on the Canadian Security Intelligence Service (CSIS) to act domestically and abroad, thus potentially resulting in mass surveillance and targeting activities that are protected under the Covenant without sufficient and clear legal safeguards... The State party should refrain from adopting legislation that imposes undue restrictions on the exercise of the rights under the Covenant. In particular, it should: Ensure its anti-terrorism legislation provides for adequate legal safeguards"

Concluding Observations on the Sixth Periodic Report of Denmark, Human Rights Committee, U.N. Doc. CCPR/C/DNK/CO/6 (15 August 2016)

"27. The Committee is concerned that the application of some of the measures used to combat terrorism may infringe the rights set forth in the Covenant. In particular, the Committee is concerned about: ...(b) section 780 of the Administration of Justice Act, which allows interception of communication by the police domestically and which may result in mass surveillance, despite the legal guarantees provided in sections 781 and 783 of the same Act...

28. The State party should clearly define the acts that constitute terrorism in order to avoid abuses. The State party should ensure that the application of such legislation is compliant with the Covenant and that the principles of necessity, proportionality and non-discrimination are strictly observed."

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

"25. ...Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being

addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate."

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

"106. ...in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.

115. While the range of subjects in the amended G 10 Act is very broadly defined, the Court observes that... a series of restrictive conditions had to be satisfied before a measure entailing strategic monitoring could be imposed. It was merely in respect of certain serious criminal acts – which reflect threats with which society is confronted nowadays and which were listed in detail in the impugned section 3(1) – that permission for strategic monitoring could be sought."

S. and Marper v. The United Kingdokm, App. Nos. 30562/04 and 30566/04, European Court of Human Rights, Judgment (4 December 2008)

"119. In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed; in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances."

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, Main Findings, 2013/2188(INI) (21 February 2014)

"14. Points out that the abovementioned concerns are exacerbated by rapid technological and societal developments, since internet and mobile devices are everywhere in modern daily life ('ubiquitous computing') and the business model of most internet companies is based on the processing of personal data; considers that the scale of this problem is unprecedented; notes that this may create a situation where infrastructure for the mass collection and processing of data could be misused in cases of change of political regime;"

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, Main Findings, 2013/2188(INI) (21 February 2014)

"5. Notes that several governments claim that these mass surveillance programmes are necessary to combat terrorism; strongly denounces terrorism, but strongly believes that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society;

6. Recalls the EU's firm belief in the need to strike the right balance between security measures and the protection of civil liberties and fundamental rights, while ensuring the utmost respect for privacy and data protection;

7. Considers that data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens; points, therefore, to the possible existence of other purposes including political and economic espionage, which need to be comprehensively dispelled;

8. Questions the compatibility of some Member States' massive economic espionage activities with the EU internal market and competition law as enshrined in Titles I and VII of the Treaty on the Functioning of the European Union; reaffirms the principle of sincere cooperation as enshrined in Article 4(3) of the Treaty on European Union, as well as the principle that Member States shall 'refrain from any measures which could jeopardise the attainment of the Union's objectives'; ...

10. Condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; stresses that privacy is not a luxury right, but is the foundation stone of a free and democratic society; points out, furthermore, that mass surveillance has potentially severe effects on freedom of the press, thought and speech and on freedom of assembly and of association, as well as entailing a significant potential for abusive use of the information gathered against political adversaries; emphasises that these mass surveillance activities also entail illegal actions by intelligence services and raise questions regarding the extraterritoriality of national laws; ...

12. Sees the surveillance programmes as yet another step towards the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies whereby any interference with suspects' fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law, promoting instead a mix of law enforcement and intelligence activities with blurred and weakened legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence; recalls in this regard the decision of the German Federal Constitutional Court on the prohibition of the use of preventive dragnets ('präventive Rasterfahndung') unless there is proof of a concrete danger to other high-ranking legally protected rights, whereby a general threat situation or international tensions do not suffice to justify such measures; ...

21. Calls on the US authorities and the EU Member States, where this is not yet the case, to prohibit blanket mass surveillance activities;

22. Calls on the EU Member States, and in particular those participating in the so-called '9-eyes' and '14-eyes' programmes', to comprehensively evaluate, and revise where necessary, their national legislation and practices governing the activities of the intelligence services so as to ensure that they are subject to parliamentary and judicial oversight and public scrutiny, that they respect the principles of legality, necessity, proportionality, due process, user notification and transparency, including by reference to the UN compilation of good practices and the recommendations of the Venice Commission, and that they are in line with the standards of the European Convention on Human Rights and comply with Member States' fundamental rights obligations, in particular as regards data protection, privacy, and the presumption of innocence."

Parliamentary Assembly of the Council of Europe (PACE), Resolution on Mass Surveillance 2045 (21 April 2015)

"2. The information disclosed so far in the Snowden files has triggered a massive, worldwide debate about mass surveillance by the intelligence services of the United States and other countries and the potential lack of adequate legal regulation and technical protection at national and international levels, and/or their effective enforcement.

3. The disclosures have provided compelling evidence of the existence of far-reaching, technologically advanced systems put in place by United States intelligence services and their partners in certain Council of Europe member States to collect, store and analyse communication data, including content, location and other metadata, on a massive scale, as well as targeted surveillance measures encompassing numerous people against whom there is no ground for suspicion of any wrongdoing.

4. The surveillance practices disclosed so far endanger fundamental human rights, including the rights to privacy (Article 8 of the European Convention on Human Rights (ETS No. 5)), freedom of information and expression (Article 10), a fair trial (Article 6) and freedom of religion (Article 9) – especially when confidential communications with lawyers and religious ministers are intercepted and when digital evidence is manipulated. These rights are cornerstones of democracy. Their infringement without adequate judicial control also jeopardises the rule of law...

8. The consequences of mass surveillance tools such as those developed by the United States and allied services falling into the hands of authoritarian regimes would be catastrophic. In times of crisis, it is not impossible for executive power to fall into the hands of extremist politicians, even in established democracies. High-technology surveillance tools are already in use in a number of authoritarian regimes and are used to track down opponents and to suppress freedom of information and expression...

19. The Assembly therefore urges the Council of Europe member and observer States to:

> 19.1. ensure that their national laws only allow for the collection and analysis of personal data (including so-called metadata) with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity; unlawful data collection and processing should be

penalised in the same way as the violation of the traditional confidentiality of correspondence; the creation of "back doors" or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses should be strictly prohibited; all institutions and businesses holding personal data should be required to apply the most effective security measures available...

19.3. provide credible, effective protection, including asylum, for whistle-blowers who expose unlawful surveillance activities and for those threatened by retaliation in their home countries, as far as possible under national law, provided their disclosures qualify for protection under the principles advocated by the Assembly...

19.5. promote the further development of user-friendly (automatic) data protection techniques capable of countering mass surveillance and any other threats to Internet security, including those posed by non-State actors;

19.6. refrain from exporting advanced surveillance technology to authoritarian regimes."

Chapter 5B: Debates Surrounding Surveillance-Related Capabilities

A. The Debate over Encryption and "Going Dark" (extended)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (17 April 2013)

"88. States should refrain from compelling the identification of users as a precondition for access to communications, including online services, cybercafés, or mobile telephony.

89. Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys."

U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017)

"...Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association...

9. Encourages business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity, and calls upon States not to interfere with the use of such technical solutions, with any restrictions thereon complying with States' obligations under international human rights law;"

Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)

"49. As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive.

50. That assessment cannot be called into question by the fact relied upon in particular by Mr Tschohl and Mr Seitlinger and by the Portuguese Government in their written observations submitted to the Court that there are several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication. Whilst, admittedly, that fact is such as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate, as the Advocate General has pointed out in paragraph 137 of his Opinion."

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Report on the US NSA surveillance programme, surveillance bodies in various Member States

and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, Main Findings, 2013/2188(INI) (21 February 2014)

"35. Notes that the companies identified by media revelations as being involved in the large-scale mass surveillance of EU data subjects by the US NSA are companies that have self-certified their adherence to the Safe Harbour, and that the Safe Harbour is the legal instrument used for the transfer of EU personal data to the US (examples being Google, Microsoft, Yahoo!, Facebook, Apple and LinkedIn); expresses its concerns that these organisations have not encrypted information and communications flowing between their data centres, thereby enabling intelligence services to intercept information; welcomes the subsequent statements by some US companies that they will accelerate plans to implement encryption of data flows between their global data centres;"

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"150. As far as freedom of expression is concerned, the violation of the privacy of communications can give rise to a direct restriction when—for example—the right cannot be exercised anonymously as a consequence of the surveillance activity. In addition, the mere existence of these types of programs leads to an indirect limitation that has a chilling effect on the exercise of freedom of expression. Indeed, the violation of the privacy of communications makes people cautious of what they say and—therefore—of what they do; it instils fear and inhibition as part of the political culture, and it forces individuals to take precautions in communicating with others. Moreover, the people most affected are those who take unpopular positions, or the members of political, racial, or religious minorities who are often unjustifiably classified as "terrorists," which makes them the object of surveillance and monitoring without proper oversight. A democratic society requires that individuals be able to communicate without undue interference, which means that their communications must be private and secure..."

B. The Debate over Hacking and Vulnerability Exploitation (extended)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/17/27 (16 May 2011)

"51. Cyber-attacks, or attempts to undermine or compromise the function of a computer-based system, include measures such as hacking into accounts or computer networks, and often take the form of distributed denial of service (DDoS) attacks... such attacks are sometimes undertaken during key political moments. The Special Rapporteur also notes that websites of human rights organizations and dissidents are frequently and increasingly becoming targets of DDoS attacks...

52. When a cyber-attack can be attributed to the State, it clearly constitutes inter alia a violation of its obligation to respect the right to freedom of opinion and expression. Although determining the origin of cyber-attacks and the identity of the perpetrator is often technically difficult, it should be noted that States have an obligation to protect individuals against interferences by third parties that undermines the enjoyment of the right to freedom of opinion and expression. This positive obligation to protect entails that States must take appropriate and

effective measures to investigate actions taken by third parties, hold the persons responsible to account, and adopt measures to prevent such recurrence in the future."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/20/17 (4 June 2012)

"63. Additionally, the Special Rapporteur is deeply concerned by harassment of online journalists and bloggers, such as illegal hacking into their accounts, monitoring of their online activities... and the blocking of websites that contain information that are critical of authorities. Such actions constitute intimidation and censorship.

64. The Special Rapporteur reiterates that the right to freedom of expression should be fully guaranteed online, as with offline content. If there is any limitation to the enjoyment of this right exercised through the internet, it must also conform to the criteria listed in article 19, paragraph 3, of the International Covenant on Civil and Political Rights. This means that any restriction imposed as an exceptional measure must (i) be provided by law, which is clear and accessible to everyone; (ii) pursue one of the legitimate purposes set out in article 19, paragraph 3, of the Covenant; and (iii) be proven as necessary and the least restrictive means required to achieved the purported aim."

Report of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/HRC/31/64 (8 March 2016)

"39. The [Special Rapporteur on the Right to Privacy] firmly encourages the three committees of the UK Parliament commended above to continue, with renewed vigour and determination, to exert their influence in order that disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the Investigatory Powers Bill be outlawed rather than legitimised. It would appear that the serious and possibly unintended consequences of legitimising bulk interception and bulk hacking are not being fully appreciated by the UK Government... SRP invites the UK Government to show greater commitment to protecting the fundamental right to privacy of its own citizens and those of others and also to desist from setting a bad example to other states by continuing to propose measures, especially bulk interception and bulk hacking, which prima facie fail the standards of several UK Parliamentary Committees, run counter to the most recent judgements of the European Court of Justice and the European Court of Human Rights, and undermine the spirit of the very right to privacy...

51. While some governments continue with ill-conceived, ill-advised, ill-judged, ill-timed and occasionally ill-mannered attempts to legitimise or otherwise hang on to disproportionate, unjustifiable privacy-intrusive measures such as bulk collection, bulk hacking, warrantless interception etc. other governments led, in this case by the Netherlands and the USA have moved more openly towards a policy of no back doors to encryption. The SRP would encourage many more governments to coalesce around this position."

Council of Europe Convention on Cybercrime, Preamble (23 November 2001)

"...Convinced that the present Convention is necessary to deter action directed against the confidentially, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this convention, and the adoption of powers sufficient for

effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation."

Parliamentary Assembly of the Council of Europe (PACE), Resolution on Mass Surveillance 2045 (21 April 2015)

"5. The Assembly is deeply worried about threats to Internet security by the practices of certain intelligence agencies, disclosed in the Snowden files, of seeking out systematically, using and even creating "back doors" and other weaknesses in security standards and implementation that could easily be exploited by terrorists and cyberterrorists or other criminals."

European Commission For Democracy Through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006 (7 April 2015)

"101. ...a signals intelligence agency, through agreement with ISPs, or even without this agreement, might be able to access stored data, e.g. in the "cloud". Here it should be stressed that even if the ISP gives its consent, for states bound by European principles of data protection, it is not possible to argue that such access does *not* involve an interference with privacy and/or freedom of correspondence. For such personal data, the interference thus occurs even if the legal "owner" or controller of the data gives its consent. Thus, it follows that statutory authority must also exist for such a power of access without consent. The same can be said for the even more controversial power of remotely hacking into computers, and planting malware. This is equivalent to a search and seizure, with the difference that it is covert and continuous throughout the period of operation of the malware, rather than open and on one occasion only. Following the ECtHR's case law on search and seizure, if this is to be allowed at all, it can only be with a very limited list of offences, with clear statutory authority, judicial authorization, minimization and destruction requirements and, bearing in mind its covert nature, strong oversight."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Concern Over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere, Press Release R80/15 (21 July 2015)

"In recent days, at least 400 GB of information were publicly exposed from the Italian firm *Hacking Team*, a company dedicated to the commercialization of the Remote Control System (RCS) spying software provided to government and government agencies... The surveillance software commercialized by the company is designed to evade computers or mobile phones' encryption, allowing the gathering of information, messages, calls and emails, voice over IP and chat communication from everyday devices. This software can also remotely activate microphones and cameras... On this disclosure, and facing possible impacts derived from the usage of this type of privacy-invading technologies and the right to exercise freedom of expression without illegal interferences, the Office of the Special Rapporteur would like to recall that according to international standards, the use of programs or systems for the surveillance of private communications should be clearly and precisely established by law, genuinely exceptional and selective, and must be strictly limited to the needs to meet compelling objectives such as the investigation of serious crime as defined in legislation. Such restrictions must be strictly proportionate and consistent with the international standards of the

right to freedom of expression. This Office has stated that the surveillance of communications and the interference in privacy that exceeds what is stipulated by law, which are oriented to aims that differ from those which the law permits or are carried out clandestinely, must be harshly punished. Such illegitimate interference includes actions taken for political reasons against journalists and independent media."

Chapter 6B: Right to Privacy and the Roles and Responsibilities of MNCs

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (17 April 2013)

"76. ...States should exercise adequate oversight in order to meet their international human rights obligations when they contract with, or legislate for, corporate actors where there may be an impact upon the enjoyment of human rights. Human rights obligations in this regard apply when corporate actors are operating abroad.

77. States must ensure that the private sector is able to carry out its functions independently in a manner that promotes individuals' human rights. At the same time, corporate actors cannot be allowed to participate in activities that infringe upon human rights, and States have a responsibility to hold companies accountable in this regard...

96. States must refrain from forcing the private sector to implement measures compromising the privacy, security, and anonymity of communications services, including requiring the construction of interception capabilities for State surveillance purposes or prohibiting the use of encryption.

97. States must take measures to prevent the commercialization of surveillance technologies, paying particular attention to research, development, trade, export and use of these technologies considering their ability to facilitate systematic human rights violations."

Parliamentary Assembly of the Council of Europe (PACE), Resolution on Mass Surveillance 2045 (21 April 2015)

"6. It is also worried about the collection of massive amounts of personal data by private businesses and the risk that these data may be accessed and used for unlawful purposes by State or non-State actors. In this context, it should be underlined that private businesses should respect human rights pursuant to the Resolution 17/4 on human rights and transnational corporations and other business enterprises, adopted by the United Nations Human Rights Council in June 2011..."

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015)

"62. While the present report does not draw conclusions about corporate responsibilities for communication security, it is nonetheless clear that, given the threats to freedom of expression online, corporate actors should review the adequacy of their practices with regard to human right norms. At a minimum, companies should adhere to principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, and the Telecommunications Industry Dialogue Guiding Principles. Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers."

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/32/38 (11 May 2016)

"85. States bear a primary responsibility to protect and respect the right to exercise freedom of opinion and expression. In the information and communication technology context, this means that States must not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal means. Any demands, requests and other measures to take down digital content or access customer information must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under article 19 (3) of the International Covenant on Civil and Political Rights. Particularly in the context of regulating the private sector, State laws and policies must be transparently adopted and implemented...

87. States place undeniable pressures on the private information and communication technology sector that often lead to serious restrictions on the freedom of expression. The private sector, however, also plays independent roles that may either advance or restrict rights, a point the Human Rights Council well understood by adopting the Guiding Principles on Business and Human Rights in 2011 as general guidance in that field. Private entities should be evaluated on the steps they take both to promote and undermine freedom of expression, even in hostile environments unfriendly to human rights.

88. Among the most important steps that private actors should take is the development and implementation of transparent human rights assessment procedures. They should develop and implement policies that take into account their potential impact on human rights. Such assessments should critically review the wide range of private sector activities in which they are engaged, such as the formulation and enforcement of terms of service and community standards on users' freedom of expression, including the outsourcing of such enforcement; the impact of products, services and other commercial initiatives on users' freedom of expression as they are being developed, including design and engineering choices, and plans for differential pricing of or access to Internet content and services; and the human rights impact of doing business with potential government customers, such as the operation of telecommunication infrastructure or the transfer of content-regulation or surveillance technologies.

89. It is also critical that private entities ensure the greatest possible transparency in their policies, standards and actions that implicate the freedom of expression and other fundamental rights. Human rights assessments should be subject to transparent review, in terms of their methodologies, their interpretation of legal obligations and the weight that such assessments have on business decisions. Transparency is important across the board, including in the context of content regulation, and should include the reporting of government requests for takedowns.

90. Beyond adoption of policies, private entities should also integrate commitments to freedom of expression into internal policymaking, product engineering, business development, staff training and other relevant internal processes."

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

"169. The service providers should be able to publicly disclose the procedures they use when they receive requests for information from government authorities, as well as information on at least the types of requests they receive and the number of requests. On this point, it bears noting that various Internet companies have adopted the practice of issuing transparency reports that disclose some aspects of the government requests for access to user information they receive."

Annex: List of Sources

I. International Treaties and Agreements

Universal Declaration of Human Rights (10 December 1948)

American Declaration on the Rights and Duties of Man (2 May 1948)

European Convention for the Protection of Human Rights and Fundamental Freedoms (4 November 1950)

International Covenant on Civil and Political Rights (16 December 1966)

American Convention ON Human Rights (Pact of San Jose) (22 November 1969)

Organization for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28 January 1981)

Convention on the Rights of the Child (20 November 1989)

International Convention on the Protection of the rights of All Migrant Workers and Members of Their Families (18 December 1990)

Charter of Fundamental Rights of the European Union (7 December 2000)

Council of Europe Convention on Cybercrime (23 November 2001)

The Arab Charter on Human Rights (22 May 2004)

Convention on the Rights of Persons with Disabilities (13 December 2006)

II. U.N. Law

International Court of Justice Case Law

Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Request for the Indication of Provisional Measures, I.C.J. Reports 2014, p. 147 (3 March 2014).

U.N. General Assembly Documents

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (18 December 2014)

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/71/199 (19 December 2016)

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (22 July 2015)

U.N. Human Rights Committee Documents

U.N. Human Rights, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (8 April 1988)

U.N. Human Rights Committee, *Toonen v. Australia*, Comm. No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (31 March 1994)

U.N. Human Rights Committee, Antonius Cornelis Van Hulst v. Netherlands, Comm. No. 903/1999, U.N. Doc. CCPR/C/82/D903/1999 (15 November 2004)

Concluding Observations of the Fourth Periodic Report of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4 (23 April 2014)

Concluding Observations on the Initial Periodic Report of Malawi, Human Rights Committee, U.N. Doc. CCPR/C/MWI/CO/1/Add.1 (19 August 2014)

Concluding Observations on the Fifth Periodic Report of Sri Lanka, Human Rights Committee, U.N. Doc. CCPR/C/LKA/CO/5 (21 November 2014)

Concluding Observations on the Seventh Periodic Report of the Russian Federation, Human Rights Committee, U.N. Doc. CCPR/C/RUS/CO/7 (28 April 2015)

Concluding Observations on the Sixth Periodic Report of Canada, Human Rights Committee, U.N. Doc CCPR/C/CAN/CO/6 (13 August 2015)

Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, Human Rights Committee, U.N. Doc. CCPR/C/MKD/CO/3 (17 August 2015)

Concluding observations on the fifth periodic report of France, Human Rights Committee, U.N. Doc. CCPR/C/FRA/CO/5 (17 August 2015)

Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (17 August 2015)

Concluding Observations on the Fourth Periodic Report of the Republic of Korea, Human Rights Committee, U.N. Doc. CCPR/C/KOR/CO/4 (3 December 2015)

Concluding Observations on the Second Periodic Report of Namibia, Human Rights Committee, U.N. Doc. CCPR/C/NAM/CO/2 (22 April 2016)

Concluding Observations on the Initial Report of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1 (27 April 2016)

Concluding Observations on the Seventh Periodic Report of Sweden, Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7 (28 April 2016)

Concluding Observations on the Sixth Periodic Report of New Zealand, Human Rights Committee, U.N. Doc. CCPR/C/NZL/CO/6 (28 April 2016)

Concluding Observations on the Fourth Periodic Report of Rwanda, Human Rights Committee, U.N. Doc. CCPR/C/RWA/CO/4 (2 May 2016)

Concluding Observations on the Sixth Periodic Report of Denmark, Human Rights Committee, U.N. Doc. CCPR/C/DNK/CO/6 (15 August 2016)

Concluding Observations on the Seventh Periodic Report of Colombia, Human Rights Committee, U.N. Doc. CCPR/AZE/CO/4 (4 November 2016) (as translated from the original Spanish)

Concluding Observations on the Sixth Periodic Report of Morocco, Human Rights Committee, U.N. Doc. CCPR/C/MAR/CO/6 (4 November 2016) (as translated from the original French)

Concluding Observations on the Seventh Periodic Report of Poland, Human Rights Committee, U.N. Doc. CCPR/C/POL/CO/7 (4 November 2016)

Concluding Observations on the Sixth Periodic Report of Italy, Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6 (28 March 2017)

Concluding Observations on the Second Periodic Report of Turkmenistan, Human Rights Committee, U.N. Doc. CCPR/C/TKM/CO/2 (28 March 2017)

Concluding Observations on the Initial Report of Pakistan, Human Rights Committee, U.N. Doc. CCPR/C/PAK/CO/1 (27 July 2017)

Concluding Observations on the Second Periodic Report of Honduras, Human Rights Committee, U.N. Doc. CCPR/C/HND/CO/2 (27 July 2017) (translated from the original Spanish)

Concluding Observations on the Fourth Periodic Report of Switzerland, Human Rights Committee, U.N. Doc. CCPR/C/CHE/CO/4 (27 July 2017) (translated from the original French)

U.N. Human Rights Council Documents

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/HRC/13/37 (28 December 2009)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/17/27 (16 May 2011)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/20/17 (4 June 2012)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (17 April 2013)

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/28/L.27 (24 March 2015)

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, U.N. Doc. A/HRC/29/32 (22 May 2015)

Report of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/HRC/31/64 (8 March 2016)

Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/32/38 (11 May 2016)

Report of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/71368 (30 August 2016)

U.N. Human Rights Council Resolution on the Safety of Journalists, U.N. Doc. A/HRC/33/L.6 (26 September 2016)

John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, Brief of Amici Curiae, United Nations Human Rights Experts in Support of Plaintiff-Appellant and Reversal, D.C. Ct. App., Case No. 16-7081 (1 November 2016)

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/HRC/34/61 (21 February 2017)

U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017)

III. European Law

European Court of Human Rights Case Law

Klass and Others v. Germany, App. No. 5029/71, European Court of Human Rights, Judgment (6 September 1978)

Malone v. The United Kingdom, App. No. 8691/79, European Court of Human Rights, Judgment (2 August 1984)

Leander v. Sweden, App. No. 9248/81, European Court of Human Rights, Judgment (26 March 1987)

Kruslin v. France, App. No. 11801/85, European Court of Human Rights, Judgment (24 April 1990)

Kopp v. Switzerland, App. No. 23224/94, European Court of Human Rights, Judgment (25 March 1998)

Rotaru v. Romania, App. No. 28341/95, European Court of Human Rights, Judgment (4 May 2000)

Taylor-Sabori v. The United Kingdom, App. No. 47114/99, European Court of Human Rights, Judgment (22 October 2002)

Weber and Saravia v. Germany, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (29 June 2006)

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, European Court of Human Rights, Judgment (28 June 2007)

Liberty and Others v. The United Kingdom, App. No. 58243/00, European Court of Human Rights, Judgment (1 July 2008)

S. and Marper v. The United Kingdokm, App. Nos. 30562/04 and 30566/04, European Court of Human Rights, Judgment (4 December 2008)

Iordachi and Others v. Moldova, App. No. 25198/02, European Court of Human Rights, Judgment (24 September 2009)

Kennedy v. The United Kingdom, App. No. 26839/05, European Court of Human Rights, Judgment (18 May 2010)

Uzun v. Germany, App. No. 35623/05, European Court of Human Rights, Judgment (2 September 2010)

Shimovolos v. Russia, App. No. 30194/09, European Court of Human Rights, Judgment (21 June 2011)

Dragojević v. Croatia, App. No. 68955/11, European Court of Human Rights, Judgment (15 January 2015)

Roman Zakharov v. Russia, App. No. 47143/06, European Court of Human Rights, Judgment (4 December 2015)

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

Sommer v. Germany, App. No. 73607/13, European Court of Human Rights, Judgment (27 April 2017)

Council of Europe

Commissioner for Human Rights, Council of Europe, Issue Paper on Democratic and Effective Oversight of National and Security Services (May 2015)

Commissioner for Human Rights, Council of Europe, Positions on Counter-Terrorism and Human Rights Protection (5 June 2015)

Parliamentary Assembly of the Council of Europe (PACE)

Parliamentary Assembly of the Council of Europe (PACE), Resolution on Mass Surveillance 2045 (21 April 2015)

European Commission for Democracy through Law (Venice Commission)

European Commission For Democracy Through Law (Venice Commission), Report on the Democratic Oversight of the Security Services, Study No. 388/2006 CDL-AD(2007)016 (11 June 2007)

European Commission For Democracy Through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006 (7 April 2015)

Court of Justice of the European Union Case Law

Digital Rights Ireland Ltd v. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung and others (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (8 April 2014)

Maximillian Schrems v. Data Protection Commissioner (C-362/14), Court of Justice of the European Union, Grand Chamber, Judgment (6 October 2015)

Patrick Breyer v. Bundesrepublik Deutschland (C-582/14), Court of Justice of the European Union, Second Chamber, Judgment (19 October 2016)

Tele2 Sverige AB v. Post- Och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Tom Watson et. al. (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (21 December 2016)

Draft agreement between Canada and the European Union on the Transfer of Passenger Name Record data (1/15), Court of Justice of the European Union, Grand Chamber, Opinion pursuant to Article 218(11) TFEU (26 July 2017)

European Parliament

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their

impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, Main Findings, 2013/2188(INI) (21 February 2014)

IV. Inter-American Law

Inter-American Court of Human Rights

Garcia v. Peru, Inter-American Court of Human Rights, Case 11.006, Report No. 1/95, OEA/Ser.L/V/II.88 (17 February 1995)

Tristán Donoso v. Panamá, Inter-American Court of Human Rights, Judgment (on Preliminary Objection, Merits, Reparations, and Costs), Series C No. 193 (27 January 2009)

Escher et al. v. Brazil, Inter-American Court of Human Rights, Judgment (on Preliminary Objection, Merits, Reparations, and Costs), Series C No. 200 (6 July 2009)

Inter-American Commission on Human Rights

Ms. X and Y v. Argentina, Inter-American Commission on Human Rights, Case 10.506, Report No. 38/96 (15 October 1996)

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (31 December 2013)

The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Concern Over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere, Press Release R80/15 (21 July 2015)