KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

INTERNATIONAL LAW AND SECRET SURVEILLANCE: BINDING RESTRICTIONS UPON STATE MONITORING OF TELEPHONE AND INTERNET ACTIVITY

9/4/2014

Sarah St.Vincent
Human Rights and Surveillance Legal Fellow

CONTENTS

I. Introduction

In the year that has followed Edward Snowden's first disclosures concerning secret US and UK surveillance practices, many governments, human-rights groups, and UN bodies have debated—and at times disagreed sharply—about whether the Internet and telephone surveillance practices that governments employ today are consistent with international law. With a view to informing these discussions, this report briefly summarizes the current state of international law as it applies to the secret surveillance of communications.

Many commentators divide international law into two categories: "hard law," which is binding upon at least some states, and "soft law," which includes nonbinding materials such as UN General Assembly resolutions. In order to facilitate a greater degree of understanding and consensus, this report is restricted to major international sources of "hard law."

The report describes two distinct bodies of law: customary international law (specifically, the principle of territorial and political integrity) and international human-rights law. As explained below, these two bodies of law exist independently of one another, meaning that a surveillance practice that does not violate human-rights law may still violate customary international law, and vice versa. The report does not address the special legal regimes that apply during situations of armed conflict.

Where international human-rights law is concerned, the report focuses on the right to privacy, freedom of expression, and the right to a remedy, and provides a summary of the applicable case-law of the European Court of Human Rights and Inter-American Court of Human Rights. In this respect, the report is intended to serve as a basic reference work for scholars, practitioners, and activists.

Although the applicability of the relevant laws and norms to the United States is described in some detail, the discussion below is relevant to all states' surveillance practices.

II. Customary International Law: The Principle of Territorial and Political Integrity

Under international law, some fundamental principles are automatically binding upon all states, regardless of whether those states have ever explicitly consented to them; these rules are known as "customary" international law ("CIL").[1] CIL is a category of law that is distinct from, and broader than, international human-rights law. A CIL norm arises where, first, states consistently behave in a way that adheres to the norm, and, second, national courts have widely and consistently expressed a view that their governments are obligated under either domestic or international law to comply with the norm.[2]

There is a general—although not universal—consensus among international-law experts that where a CIL norm has come into existence, a state will only avoid being bound by it if that state

[1] *See* North Sea Continental Shelf Cases (Ger. v. Den.; Ger. v. Neth.), Judgment, 1969 I.C.J. 72, paras. 37-38 (Feb. 20).

[2] *Ibid.*

has persistently objected to the norm as that norm has emerged, and if the norm is of a kind that is susceptible to derogation.[3] (Some commonly cited examples of norms that are not susceptible to derogation—that is, rules to which a state can never validly object—are the customary prohibitions on slavery and torture.)

This means that although some human-rights obligations are so widely accepted by states that they rise to the level of customary law, CIL constitutes a separate body of legal norms and applies to all states regardless of whether they have signed any treaty or how they might interpret a treaty's provisions (unless the norm in question is susceptible to derogation and the state has persistently objected to it).[4] In other words, a state's actions may violate CIL even if they do not violate a human-rights treaty or other international agreement. Thus, a state whose surveillance practices violate a customary norm is breaking the law, even if that state has never signed a human-rights treaty.

One of the most fundamental and widely recognized CIL norms requires all states to respect one another's territorial and political integrity; this requirement applies not only to a state's physical incursions into another state's territory, but also to its interference with another state's internal or external affairs.[5] As the International Court of Justice ("ICJ") has explained, a state violates this customary law when it uses some form of coercion in order to intervene, either directly or indirectly, in matters that another state has the right to determine for itself.[6] Although armed violence is one clear form of coercion, the ICJ's discussion of this rule suggests that it may be possible for a state to use "coercion" in this context without using, or threatening to use, force.[7] A 1970 UN General Assembly resolution that the ICJ views as declarative of CIL confirms this interpretation of the requirement, referring to "the duty of States to refrain in their international relations from military, political, economic or any other form of coercion aimed against the political independence or territorial integrity of any State" and asserting:

No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of

---

[3] *See* Michael Byers, *Custom, Power, and the Power of Rules: Customary International Law from a Multidisciplinary Perspective*, 17 MICH. J. INT'L L. 109, 163 (1995); Dinah Shelton, *Normative Hierarchy in International Law*, 100 AM J. INT'L L. 291, 297-305 (2006).

[4] An example of a human-rights obligation that is codified in treaties, but also qualifies as a CIL norm, is the prohibition on torture. *See generally* International Committee of the Red Cross, Rule 90. Torture and Cruel, Inhuman or Degrading Treatment, http://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule90 (last accessed Aug. 18, 2014).

[5] Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment (Merits), 1986 I.C.J. 160, para. 202 (June 27); *see also* Corfu Channel (U.K. v. Alb.), Judgment (Merits), 1949 I.C.J. 4, 35 (April 9).

[6] *Id*. at para. 205.

[7] *Id*.

the State or against its political, economic and cultural elements, are in violation of international law.[8]

The question of whether a state, by clandestinely monitoring communications that were sent or received in another state, violates these binding principles of law has not yet been fully explored by courts. The European Court of Human Rights ("ECtHR")—the only international court that has addressed this question explicitly, even in passing—found that Germany's interception of signals or data originating abroad did not violate the CIL norm of territorial sovereignty where the relevant interception or collection facilities were located on German soil and the data collected were subsequently used only in Germany.[9] In reaching this finding, the ECtHR indicated that Germany would have had to undertake some form of extraterritorial action in order for a violation of territorial sovereignty to occur.[10]

Meanwhile, the ICJ jurisprudence cited above, particularly the Military and Paramilitary Activities judgment, suggests that if a state does engage in coercive interference with some aspect of communications that occurs outside of its borders, that state may be violating CIL. In other words, the legality of a state's clandestine surveillance of communications, insofar as it takes place within or touches upon the territory of another state, may depend on whether those surveillance practices constitute an "interference" with communications or some other aspect of the other state's internal affairs or infrastructure, as well as whether the interferences are "coercive." (The concept of "interference" in this context should be distinguished from the notion under human rights law of interference with an individual's right to privacy; for a discussion of the latter type of interference, see below.)

III. International Human Rights Law: Scope of the Treaties and Application within the United States

This report's discussion of human rights is primarily concerned with the International Covenant on Civil and Political Rights ("ICCPR"), the European Convention on Human Rights ("ECHR," officially titled the Convention for the Protection of Human Rights and Fundamental Freedoms), the American Convention on Human Rights ("ACHR"), and the American Declaration of the Rights and Duties of Man ("American Declaration").

---

[8] Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. Doc. A/RES/25/2625 (Oct. 24, 1970) (emphasis added); Military and Paramilitary Activities, *supra* note 5, at paras. 191-92; *see also* Douwe Korff, *Expert Opinion prepared for the Committee of Inquiry of the Bundestag into the "5EYES" global surveillance systems revealed by Edward Snowden* (June 5, 2014), p. 4-7, *available at* http://www.statewatch.org/news/2014/jun/snowden-korff-expert-opinion-bundestag-June-2014.pdf (last visited June 25, 2014).

[9] Weber and Saravia v. Germany, App. No. 54934/00, Decision (Admissibility), 2006-XI Eur. Ct. H.R. 1173, paras. 87-88 (The Court did not address this question in Liberty v. United Kingdom, App. No. 58243/00, Judgment, 2008 Eur. Ct. H.R. 568.).

[10] Weber v. Germany, *supra* note 9; *see also* Öcalan v. Turkey, App. No. 46221/99, Judgment (Grand Chamber), 2005-IV Eur. Ct. H.R. 282, para. 90.

A. Applicability of human-rights treaties to the United States

The United States has signed and ratified the ICCPR, meaning that it is bound by the treaty at an international level; however, it has not passed legislation of the kind that would give the treaty effect in domestic law, meaning that litigants cannot rely directly upon the treaty's provisions in US courts.[11] Meanwhile, the US has signed, but not ratified, the ACHR, meaning that it is not bound by that document. However, the country has signed and ratified the Charter of the Organization of American States, and therefore—in the view of the Inter-American Commission on Human Rights—it is bound at the international level by the American Declaration.[12] The Inter-American Commission has resolved a number of cases against the United States on the basis of the Declaration.[13]

The ECHR applies only within the Council of Europe Member States and does not have any legal effect upon the United States at either the domestic or international level, although it is the source of the best-developed body of international human-rights case law where surveillance is concerned.

B. Extraterritorial scope of the treaties

The extent to which states are bound by any of the aforementioned treaties with respect to individuals beyond their own borders has not yet been fully settled. In its advisory opinion in *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, the ICJ considered the scope of the jurisdictional provision of the ICCPR, which states at Article 2(1) that "[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant." The Court concluded that the ICCPR "is applicable in respect of acts done by a State in the exercise of its jurisdiction outside its own territory," and has subsequently reaffirmed this position in the contentious case of *Armed Activities on the Territory of the Congo*.[14] However, the Court has not yet set out criteria for determining when a state is exercising its jurisdiction, or whether a state may be liable under the ICCPR for effects it creates in areas beyond that jurisdiction.

The equivalent provision of the ECHR (Article 1) obligates states parties to "secure to everyone within their jurisdiction the rights and freedoms" set out in the Convention. The ECtHR's case-law establishes that although "[a] State's jurisdictional competence under [the Convention] is

---

[11] On the need for such legislation before a treaty can be binding as a matter of domestic law (unless the treaty is self-executing), see Medellín v. Texas, 552 U.S. 491, 498-99 (2008). Being bound at an international level means that the state has accepted that the obligation in question applies to its relations with other states; in some circumstances, it can also mean that an individual (or another state) can bring a case against the state in an international court.

[12] *See* Roach v. United States, Case 9647, Inter-Am. Comm'n H.R., Resolution No. 3/87, OEA/Ser.L/V/II.71, doc. 9 rev.1 ¶¶ 46-49 (1987). The fact that the U.S. responds to actions against it before the IACHR suggests that it accepts that the American Declaration binds the country internationally; see *infra* note 13 and accompanying text.

[13] *See*, *e.g.*, Lenahan (Gonzalez) v. United States, Case 12.626, Inter-Am. Comm'n H.R., Report No. 80/11 (2011); Coard v. United States, Case 10.951, Inter-Am. Comm'n H.R., Report No. 109/99, OEA/Ser.L/V/II.106, doc. 6 rev. (1999).

[14] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, para. 111; Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 216.

primarily territorial," there are at least a few "exceptional" circumstances in which the state may be liable under the Convention for events occurring outside its territory.[15] A clear example arises where, as a result of military action, a state "exercises effective control of an area outside [its] national territory."[16] Another example occurs where a state's agent exerts authority and control over an individual in a foreign territory, or where the state "exercises all or some of the public powers normally to be exercised by [another] Government."[17] Examples include situations in which a state's agents (such as law-enforcement authorities or military personnel) take an individual into custody in another state, or when a state exercises control over an overseas detention facility or a ship in international waters.[18] However, the Court has not yet issued a ruling on the scope of the Convention's applicability to a state's foreign surveillance activities.[19]

The jurisdictional provision of the ACHR (Article 1) resembles a hybrid of the ICCPR and ECHR provisions, stating in relevant part: "States Parties to this Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction the free and full exercise of those rights and freedoms." The Inter-American Court of Human Rights ("IACtHR") has summarized its views regarding the extraterritorial application of the Convention as follows:

Even though a State's duty to protect the rights of any person is based on its territory, that duty may, under given circumstances, refer to conduct with an extraterritorial locus where the person concerned is present in the territory of one State, but subject to the control of another State, usually through the acts of the latter's agents abroad. In these cases, the inquiry turns on whether the alleged victim was subject to the authority and control of the acting State.[20]

The American Declaration does not contain a jurisdictional provision.

From the foregoing, it can be seen that a state's extraterritorial obligations under international human-rights treaties generally hinge on whether the individual or territory in question falls within that state's *de jure* or *de facto* "jurisdiction," "authority," or "control."[21] However, the courts have not yet adequately defined these terms, and the applicability of the treaty rights to

---

[15] Al-Skeini v. United Kingdom, App. No. 55721/07, Judgment (Grand Chamber), 2011 Eur. Ct. H.R. 1093, paras. 131-32.

[16] *Id*. at para. 138.

[17] *Id*. at paras. 134-37.

[18] *Id*.

[19] In Weber v. Germany, *supra* note 9, the Court did not reach this issue, while in Liberty v. United Kingdom, *supra* note 9, the absence of any jurisdictional discussion in the Court's judgment suggests that the question was not raised by any of the parties.

[20] Petition (Admissibility) P-900-08, Ameziane v. United States, Inter-Am. Comm'n H.R., Report No. 17/12, ¶ 30 (2012); *see also* Coard, *supra* note 13, para. 37.

[21] For a more extensive discussion of the development of international bodies' approaches to the question of extraterritorial obligations under human-rights law, see Sarah H. Cleveland, *Embedded International Law and the Constitution Abroad*, 110 COLUM. L. REV. 225, 248-270 (2010).

individuals whose communications have been monitored by a foreign state remains undetermined.[22]

C. International Human Rights Law: Substantive Rights

Although there are other rights that secret surveillance may affect, such as the right to peaceful assembly, the discussion below focuses on the three rights to which surveillance poses the most obvious and immediate risks: the right to privacy (or "private life"), the right to freedom of expression, and the right to a remedy. The relevant textual provisions of the treaties are described first, followed by the case-law of the ECtHR and IACtHR.

D. The right to "privacy" or "private life"

1. The text of the relevant documents

The ICCPR, ECHR, ACHR, and American Declaration all provide for a qualified right to "privacy" or "private life."[23]

The ICCPR provides at Article 17 that no one shall be subjected to "arbitrary or unlawful interference" with his or her "privacy" or correspondence, and that "[e]veryone has the right to the protection of the law against such interference."

The ECHR establishes a similar right in more detailed terms at Article 8, stating that "[e]veryone has the right to respect for his private … life" and correspondence, and that:

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 well-being 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.

The ECtHR has clarified that a state's interference with the right to respect for private life and correspondence "will be considered 'necessary in a democratic society' for a legitimate aim if it answers a pressing social need and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient."[24]

Much like the ICCPR, the ACHR mandates at Article 11 that no one shall be subject to "arbitrary or abusive interference" with his or her private life or correspondence, and that "[e]veryone has

[22] Sources of "soft" international law are beyond the scope of this report; however, for an assertion that many of a state's foreign surveillance activities will necessarily involve the exercise of that state's jurisdiction (and thus obligate the state to comply with its human-rights obligations), see Office of the U.N. High Comm'r for Human Rights, *The right to privacy in the digital age*, ¶ 34, U.N. Doc. A/HRC/27/37 (June 30, 2014).x

[23] The African Charter on Human and Peoples' Rights does not include a provision concerning privacy rights, although the African Charter on the Rights and Welfare of the Child does include such a provision at Article 10. *See* African Charter on the Rights and Welfare of the Child art. 2, *opened for signature* July 11, 1990, OAU Doc. CAB/LEG/24.9/49 (entered into force Nov. 29, 1999).

[24] S. and Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04, Judgment (Grand Chamber), 2008 Eur. Ct. H.R. 1581, para. 101 (most internal quotes omitted).

the right to the protection of the law against such interference." The American Declaration provides nearly identical protections at Articles 5 and 10, recognizing "the right to protection of the law against abusive attacks" upon private life and "the right to the inviolability and transmission of … correspondence."

Some common features of these different sets of provisions include:

With the exception of the American Declaration, they all use the term "interference" to describe the prohibited action. None of them make a textual distinction between types of interference.

Three of the four documents include some form of legality requirement, such that any interference with private life, correspondence, etc., must be in accordance with existing laws. (The American Declaration is once again the exception to this pattern.)

Three of the four documents (all save for the ECHR) explicitly impose a further requirement upon states to enact laws that protect individuals from illegal interferences with their privacy or private life. In other words, these treaties appear to require states not only to enact laws that govern intrusions into privacy, but also to ensure that they have adopted laws that prevent illegal interferences and/or provide victims of such interferences with some means of redress. Although this requirement is not apparent on the face of the text of the ECHR, the ECtHR has found that any surveillance program a state may adopt must include "adequate and effective guarantees against abuse."[25]

In all four documents, the right to privacy or private life is qualified rather than absolute, such that state action intruding on individuals' privacy is permissible under some circumstances.

However, the ICCPR, ACHR, and American Declaration all prohibit interferences that are "arbitrary" (ICCPR and ACHR) or "abusive" (AHCR and American Declaration), while the ECHR prohibits those that are not "necessary in a democratic society" for certain specified reasons such as public safety.

2. Jurisprudence

Under the jurisprudence of the ECtHR and the IACtHR, it is clear that the targeted surveillance of an individual can constitute a violation of the right to private life if that surveillance is abusive or unnecessary, or fails to accord with domestic law.[26] Both courts have considered the legality of surveillance that is clandestine, although research indicates that only the ECtHR has considered the lawfulness of secret surveillance programs as a whole.

a. The European Court of Human Rights

[25] Klass v. Germany, App. No. 5029/71, Judgment, 28 Eur. Ct. H.R. 4, para. 50 (1978). However, under the ECtHR's jurisprudence, these guarantees against abuse need not be codified in the same set of laws that govern the surveillance program; see Silver v. United Kingdom, App. Nos. 5947/72 et al., Judgment, 61 Eur. Ct. H.R. 11, para. 90 (1983).

[26] *See*, *e.g.*, Ortiz v. Guatemala, Case 10.526, Inter-Am. Comm'n H.R., Report No. 31/96 (1996), ¶¶ 115-116; Shimovolos v. Russia, App. No. 30194/09, Judgment, 2011 Eur. Ct. H.R. 987, paras. 65-71.

The ECtHR's case-law concerning secret surveillance programs is extensive, and addresses both the legal bases and actual conduct of the programs that a number of states have operated. Several key aspects of this jurisprudence are discussed below.

1) Interference with correspondence in the secret-surveillance context: the basic parameters

The ECtHR has found that for the purposes of the European Convention, even the "mere existence of legislation allowing secret surveillance" constitutes an interference with private lifesuch that the necessity and legality requirements of Article 8 (see below) must be met.[27] Additionally, it has found that the interception of data by public authorities constitutes interference with the right to respect for private life, just as the use, sharing, and storage of that data do.[28]

Where the data itself is concerned, e-mail, telephone, and facsimile correspondence, as well as personal information pertaining to Internet usage, all fall within the ambit of Article 8 (with the number dialed and the date and duration of the conversation being essential elements of any telephone correspondence, in addition to the conversation itself).[29] This correspondence need not be purely personal: business or professional correspondence may constitute part of an individual's private life, as can information that has previously been made public (at least in so far as the authorities systematically collect and store it).[30]

2) Necessity

The degree of necessity that the Court requires in order for a secret-surveillance measure to be lawful under Article 8 is somewhat unclear under the current jurisprudence. In at least one case, the Court has stated that secret surveillance is "tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."[31] In an older case, however, it suggested that a balancing test is at least sometimes involved when determining whether a surveillance measure is necessary in order to achieve a legitimate aim: specifically, the Court opined that the nature of the aim should be weighed against the type and seriousness of the interference with the individual's private life.[32]

---

[27] Lenev v. Bulgaria, App. No. 41452/07, Judgment, 2012 Eur. Ct. H.R. 2002, para. 144; Klass v. Germany, *supra* note 25, para. 41; Weber v. Germany, *supra* note 9, para. 78.

[28] Weber v. Germany, *supra* note 9, para. 79; Amann v. Switzerland, App. No. 27798/95, Judgment (Grand Chamber), 2000-II Eur. Ct. H.R. 88, paras. 65, 69-70; S. and Marper v. United Kingdom, *supra* note 24, para. 67.

[29] Copland v. United Kingdom, App. No. 62617/00, Judgment, 2007-I Eur. Ct. H.R. 253, paras. 43-44; Liberty v. United Kingdom, *supra* note 9, para. 56; Malone v. United Kingdom, App. No. 8691/79, Judgment, 82 Eur. Ct. H.R. 10, para. 64; Klass v. Germany, *supra* note 25, para. 41.

[30] Rotaru v. Romania, App. No. 28341/95, Judgment, 2000-V Eur. Ct. H.R. 192, para. 43; Kopp v. Switzerland, App. No. 23224/94, Judgment, 1998-II Eur. Ct. H.R. 18, para. 50; Shimovolos v. Russia, *supra* note 26, paras. 64-65.

[31] Rotaru v. Romania, *supra* n. 30, para. 47.

[32] Leander v. Sweden, App. No. 9248/81, Judgment, 116 Eur. Ct. H.R. 4, para. 59 (1987).

3) The legality requirement

According to the Court, surveillance measures must have "some basis in domestic law" in order to be "in accordance with the law" for the purposes of Article 8, and the measures must also be in accord with public international law (which includes customary international law).[33] As the Court has confirmed, having a basis in domestic law means being expressed in a binding law, and not simply in a policy.[34] Specifically, "because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance," the law must, in published statutes, set out at least:

- "the nature, scope and duration of the possible measures";
- the grounds on which the authorities can order surveillance (e.g., the relevant types of suspected criminal offences);
- which authorities have the power to order, allow, conduct, or supervise the surveillance;
- a limit on the duration of the 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";
- the circumstances in which the data will be destroyed; and
- the applicable remedy for violations or abuses.[35]

Overall, surveillance measures will only be "in accordance with the law" if those laws are accessible to individuals and if their consequences are foreseeable; that is, "[t]he 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 engage in secret surveillance, although policies that do not have the status of law may be relevant to determining whether the surveillance and its consequences are foreseeable.[36] Even where a domestic law confers discretion in respect of surveillance, this discretion cannot be unfettered, and the law must explain the scope and manner of the monitoring with sufficient clarity to protect against the arbitrary exercise of the power.[37] These explanations of the limits on surveillance-related discretion must be made in the law itself rather than merely in a policy document.[38]

---

[33] Weber v. Germany, *supra* note 9, paras. 87-88; Shimovolos v. Russia, *supra* note 26, para. 67.

[34] *See* Malone v. United Kingdom, *supra* note 29, para. 87. The Court's most recent jurisprudence consistently requires that the surveillance have a basis in statutes, and it has repeatedly listed a number of specific aspects of a surveillance program that must be codified in statutory law (see *infra* note 35 and accompanying text). However, see Huvig v. France, App. No. 11105/84, Judgment, 176 Eur. Ct. H.R. 9, para. 28 (1990), and Kruslin v. France, App. No. 11801/85, 176 Eur. Ct. H.R. 10 (1990), para. 29, finding that case-law can constitute "law" for at least some purposes that are relevant to surveillance.

[35] Shimovolos v. Russia, *supra* note 26, para. 68; Weber v. Germany, *supra* note 9, para. 95; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, Judgment, 2007 Eur. Ct. H.R. 533, para. 76.

[36] Liberty v. United Kingdom, *supra* note 9, para. 59; Malone v. United Kingdom, *supra* note 26, para. 67; Leander v. Sweden, *supra* n. 32, para. 51.

[37] Malone v. United Kingdom, *supra* note 29, paras. 68, 81; Bykov v. Russia, App. No. 4378/02. Judgment (Grand Chamber), 2009 Eur. Ct. H.R. 441, para. 78; Klass v. Germany, *supra* note 25, para. 49.

[38] Leander v. Sweden, *supra* note 32, para. 51; Malone v. United Kingdom, *supra* note 29, para. 68; Bykov v. Russia, *supra* note 37, para. 78.

As noted above, the surveillance program must include "adequate and effective guarantees against abuse," although the state is not required to confirm that any particular individual has been monitored.[39]

4) Supervision of surveillance programs

Another element that the ECtHR has made clear must be present in a surveillance program in order for it to conform to the Convention is independent supervision. In this respect, the Court has suggested that judicial oversight is "in principle desirable" in light of the ease with which such programs can be abused; however, it has stopped short of requiring judicial oversight in all circumstances.[40] Regarding a German program, for example, it found that oversight was sufficient where the reviewing bodies, which were non-judicial, were nevertheless "independent of the authorities carrying out the surveillance" and "vested with sufficient powers and competence to exercise an effective and continuous control."[41] However, the Court continues to maintain that supervision "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."[42]

5) Notification of the target(s)

The Court has found that the Contracting Parties to the ECHR are not required to disclose that they have ordered or conducted surveillance in a particular instance (at least when the surveillance is domestic and is part of a program that has been established by law), nor are they required under all circumstances to notify *post hoc* any person whom they have monitored.[43] However, the Court has clarified that after the surveillance has ended, the authorities "should" issue such a notification to an individual who has been secretly monitored, at least where they are able to do this "without jeopardising the purpose of the surveillance."[44]

6) Content and metadata

Recent disclosures have drawn attention to the fact that some governments may be seeking to draw a legal distinction between the collection of "metadata" and content. "Metadata" is generally understood as data that describe the communication in question, such as the date, time, sender, recipient, and subject line of an e-mail, or the date, time, sender, recipient, and duration of a telephone call. As discussed below, the Court has made it clear that a state's collection of metadata constitutes an interference with the right to private life. However, it is not entirely clear whether the ECtHR may regard some types of metadata as subject to a somewhat lesser degree of protection under Article 8 than content.

---

[39] Klass v. Germany, *supra* note 25, para. 50; Weber v. Germany, *supra* note 9, para. 135.

[40] Klass v. Germany, *supra* note 25, para. 56.

[41] *Id*.

[42] Rotaru v. Romania, *supra* note 30, para. 59.

[43] Klass v. Germany, *supra* note 25, para. 58.

[44] Ass'n for Eur. Integration and Human Rights v. Bulgaria, *supra* note 35, para. 90.

In the most relevant case, *Malone v. the United Kingdom*, the Court distinguished telephone "metering" (i.e., the creation of a record of numbers dialed and the time and duration of the calls) from the interception of conversations: as the Court observed, telephone companies engage in metering as a matter of course for billing and other business purposes, whereas "the interception of communications" is necessarily "undesirable and illegitimate in a democratic society unless justified."[45] However, the Court also confirmed that metadata of the kind recorded through metering is an "integral element in … communications made by telephone," such that a company's release of this metadata to law enforcement authorities constitutes an interference with the right to private life under Article 8.[46] The Court's subsequent case-law has confirmed that "metering … does not *per se* offend against Article 8 if, for example, done by the telephone company for billing purposes," but that the transmission of this information to law enforcement constitutes an interference with the right.[47] Therefore, it appears that the Court views the capturing of metadata as something that does not automatically constitute an interference with the right to private life—as the interception of the content of a conversation does—but that nevertheless is subject to the same legal analysis under Article 8 as any other form of interference in communications.

7) Specific characteristics of lawful and unlawful programs

As the ECtHR has considered the legality of various government surveillance programs, it has described the features of each program in some detail, noting those features that bolster the legality of the program and those that tend to make it illegal. It is therefore possible to list a number of specific characteristics of programs that the Court has found to be lawful or unlawful. The Court seems to apply a totality of the circumstances test; therefore, the presence of any one of these characteristics does not necessarily constitute by itself the basis for a finding of legality (or illegality) under Article 8.

Key characteristics of the secret surveillance regimes that the ECtHR has previously found to be compliant with Article 8 include the following, among others:

- The surveillance was undertaken pursuant to, and complied with, laws adopted by the state's national legislature;[48]
- The legislation "define[d] precisely, and thereby limit[ed], the purposes for which" the surveillance could be undertaken, e.g., imminent threats to public order;[49]
- These stated purposes of the surveillance program were indeed its true purposes, and not merely a pretext;[50]
- The laws governing the surveillance program provided that an individual's communications could only be monitored where there were factual grounds for believing that the individual was planning to commit (or had committed) a serious criminal offense, and where it would

[45] Malone v. United Kingdom, *supra* note 29, para. 84.

[46] *Id*.

[47] P.G. and J.H. v. United Kingdom, App. No. 44787/98, Judgment, 2001-IX Eur. Ct. H.R. 550, para. 42; *cf.* Copland v. United Kingdom, *supra* note 29, para. 43.

[48] Klass v. Germany, *supra* note 25, para. 43; Weber v. Germany, *supra* note 9, paras. 85, 90-91.

[49] Klass v. Germany, *supra* note 25, para. 45.

[50] *Id.* at para. 46.

be at least "considerably more difficult" to establish the facts relating to the crime in some other way;[51]

- The laws otherwise specified the types of suspected criminal offenses that could lead to a surveillance order (although an exhaustive enumeration of these offences is not legally required, as per the Court's jurisprudence);[52]
- The laws provided that the surveillance would be restricted to the individual in question, except where the facts clearly indicated that someone else was receiving or forwarding communications on that individual's behalf (in which case the person who received or forwarded the communications could also be monitored);[53]
- Only the heads of certain government entities had the power to request surveillance, and they could only do so in writing; or, more generally, "there was an administrative procedure designed to ensure that [surveillance] measures were not ordered haphazardly, irregularly or without due and proper consideration";[54]
- The surveillance could only be authorized for three months, at which time it could only be re-authorized if a fresh request was made;[55]
- The authorities conducting the surveillance were overseen by current or former members of the judiciary and/or a panel of democratically-elected representatives (including members of the opposition);[56]
- The law required that any information or documents obtained through surveillance measures be destroyed as soon as their retention was no longer necessary in order to pursue one of the aims described in the legislation, and that such information or documents could not be used for any other purpose;[57]
- The law set limits concerning the sharing of information between authorities;[58]
- Although judicial recourse was not available to individuals whose communications had been monitored, "bodies appointed by the people's elected representatives" (including members of the opposition) undertook a subsequent review of the surveillance;[59]
- Although individuals who had been monitored were not notified of this fact, those who believed that their communications had been (or were being) monitored could ask these bodies to undertake a review;[60] and/or
- These review bodies were independent in the sense that government agents or entities could not instruct them as to what to do.[61]

---

[51] *Id.* at para. 51; *see also* Weber v. Germany, *supra* note 9, para. 115.

[52] Weber v. Germany, *supra* note 9, para. 96; Kennedy v. The United Kingdom, App. No. 26839/05, 2010 Eur. Ct. H.R. 682, para. 159.

[53] Klass v. Germany, *supra* note 25, paras. 17, 51; *cf.* Weber v. Germany, *supra* note 9, para. 97.

[54] Klass v. Germany, *supra* note 25, para. 51; Weber v. Germany, *supra* note 9, para. 115.

[55] Klass v. Germany, *supra* note 25, para. 52; Weber v. Germany, *supra* note 9, para. 98.

[56] Leander v. Sweden, *supra* note 32, paras. 64-65; Kennedy v. The United Kingdom, *supra* note 52, para. 166; *see also* Weber v. Germany, *supra* note 9, para. 117

[57] Klass v. Germany, *supra* note 25, para. 52; *cf.* Weber v. Germany, *supra* note 9, paras. 99-100, and Kennedy v. The United Kingdom, *supra* note 52, para. 164.

[58] Klass v. Germany, *supra* note 25, para. 52; Weber v. Germany, *supra* note 6, para. 99; Kennedy v. The United Kingdom, *supra* note 52, para. 163.

[59] Klass v. Germany, *supra* note 25, paras. 53, 56.

[60] *Id.* at para. 53; Leander v. Sweden, *supra* note 32, para. 66; Kennedy v. The United Kingdom, *supra* note 52, para. 167.

Meanwhile, characteristics of secret surveillance regimes that have led the Court to find violations of Article 8 include:

- The relevant laws did not clearly indicate that a warrant was required in order for the authorities to monitor communications;[62]
- The laws did not provide a clear and exclusive list of purposes for which the authorities could undertake surveillance;[63]
- The laws did not set a limit upon the amount of time for which surveillance measures could be authorized;[64]
- The state's procedures for selecting, using, storing or retaining, and/or discarding intercepted material had not been disclosed to the public (or had not been disclosed with sufficient clarity);[65]
- There were "no legal rules concerning the scope and manner of exercise of the discretion enjoyed by public authorities" when requesting or compelling other entities to produce communications-related information (such as the length of telephone calls and the numbers dialed);[66]
- Overall control of the surveillance program was vested solely in a political appointee who was a member of the executive branch, or in a body that otherwise was not independent of the executive, or in a parliamentary body whose supervisory procedures were not set out by law;[67]
- Although requiring warrants, the laws nevertheless permitted the wholesale monitoring of "very broad classes of communications" amongst a very large number of individuals, with the practical effect that "[t]he legal discretion granted to the executive for the physical capture of external communications was … virtually unfettered";[68]
- Similarly, laws permitting wholesale monitoring also granted the authorities "wide discretion" concerning the specific communications that they could choose to read (or to which they could choose to listen);[69]
- The laws did not provide for any review of the implementation of the surveillance measures by an entity outside of the services that were conducting the surveillance, or even by a qualified and independent entity within those services;[70]

---

[61] Klass v. Germany, *supra* note 25, para. 53.

[62] Malone v. The United Kingdom, *supra* note 29, paras. 71-80.

[63] *Id.*

[64] Iordachi v. Moldova, App. No. 25198/02, 2009 Eur. Ct. H. R. 256, para. 45.

[65] *Ibid.* at para. 48; Liberty v. the United Kingdom, *supra* note 9, paras. 66-70; Amann v. Switzerland, *supra* note 28, paras. 76, 80.

[66] Malone v. the United Kingdom, *supra* note 29, para. 87.

[67] Ass'n for Eur. Integration and Human Rights v. Bulgaria, *supra* note 35, para. 87; Iordachi v. Moldova, *supra* note 64, para. 49; Popescu v. Romania (No. 2), App. No. 71525/01, 2007 Eur. Ct. H. R. 261 (2007), paras. 70-73.

[68] Liberty v. the United Kingdom, *supra* note 9, para. 64.

[69] *Id.* at para. 65.

[70] Ass'n for Eur. Integration and Human Rights v. Bulgaria, *supra* note 35, para. 85; *see also* Popescu v. Romania, *supra* note 67, paras. 74-77.

- The laws did not provide adequate guarantees concerning the confidentiality of the information obtained through surveillance, or adequate regulations governing its destruction;[71]
- The laws did not provide for the notification of subjects of surveillance measures at any time or under any circumstances whatsoever;[72] and/or
- The laws failed to provide adequate precautions to prevent the unnecessary monitoring of individuals who had merely communicated "fortuitously" with someone who was the target of surveillance (e.g., a salesperson whose contact with the target occurred through mere happenstance).[73]

b. The Inter-American Court of Human Rights

Although the IACtHR's jurisprudence concerning communications surveillance is not as robust as the ECtHR's, the Court has had at least two opportunities to consider the lawfulness of telephone wiretapping programs under Article 11 of the ACHR. In doing so, it has concluded as follows:

- In order to be non-abusive and non-arbitrary, any state restrictions on the right to privacy must "serve a legitimate purpose, and meet the requirements of suitability, necessity, and proportionality which render [them] necessary in a democratic society."[74]
- Furthermore, there is a legality requirement, meaning that restrictions on the right to privacy must be "statutorily enacted."[75]
- Telephone conversations, including both private and business-related conversations, fall within the ambit of Article 11, such that the interception of telephone communications without the consent of the callers constitutes an interference with the right to privacy.[76]
- The protected aspects of telephone conversations include not only their content, but also related information such as the initiator, recipient, time, and duration of a call.[77]
- Any law authorizing the interception of telephone communications "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."[78]
- Under at least some circumstances, a public official's disclosure of a private telephone conversation can interfere with the right to privacy.[79]

---

[71] Ass'n for Eur. Integration and Human Rights v. Bulgaria, *supra* note 35, para. 86.

[72] *Id.* at para. 91.

[73] Amann v. Switzerland, *supra* note 28, para. 61.

[74] Donoso v. Panama, Judgment, Inter-Am. Ct. H. R. (ser. C), No. 193, ¶ 56 (Jan. 27, 2009).

[75] *Id.* at para. 56; Escher v. Colombia, Judgment, Inter-Am. Ct. H. R. (ser. C), No. 200, ¶ 130 (July 6, 2009).

[76] Donoso v. Panama, *supra* note 74, ¶ 55; Escher v. Colombia, *supra* note 75, ¶ 114, 129.

[77] Escher v. Colombia, *supra* note 75, ¶ 114.

[78] *Id.* at ¶ 131.

[79] Donoso v. Panama, *supra* note 74, ¶ 76.

E. The right to freedom of expression

1. The text of the relevant documents

The ICCPR, ACHR, and ECHR all recognize a qualified right to freedom of expression.[80] The relevant provisions of the EHCR (Article 10) and ACHR (Article 13) closely track the ICCPR, which establishes at Article 19 that:

-
- *(2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
-
- *(3) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*

    - (a) For respect of the rights or reputations of others;
    - (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Under Article 10(2) of the ECHR, the qualification of the right is delimited in somewhat greater detail:

The exercise of these freedoms [i.e., to hold opinions and to receive and impart information and ideas without interference], since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Meanwhile, the ACHR includes a unique provision at Article 13(3) stating that:

The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.

Finally, the American Declaration provides at Article 4 that "[e]very person has the right to freedom of investigation, of opinion, and of the expression and dissemination of ideas, by any medium whatsoever."

[80] The African Commission on Human and Peoples' Rights has adopted a non-binding Declaration of Principles on Freedom of Expression in Africa.

2. Jurisprudence

The ECtHR has considered the potential impact of surveillance upon the right to freedom of expression in only a handful of cases. In *Weber and Saravia v. Germany*, it emphasized the importance of freedom of the press and accepted, in essence, that the existence of legislation permitting secret surveillance constituted an interference with journalists' freedom of expression.[81] Like interferences with the right to private life, interference with the right to freedom of expression—in the ECtHR's view—must be prescribed by law and necessary in a democratic society.[82] In *Weber and Saravia*, the Court found that the German legislation in question met these requirements, and that Germany therefore had not violated the applicant journalist's rights under Article 10.[83] By contrast, the Court has recently found in *Youth Initiative for Human Rights v. Serbia* that Serbia violated Article 10 when its authorities refused to disclose basic factual information about a secret surveillance program—namely, the number of people whose communications the Serbian intelligence agency had electronically monitored in 2005—to a non-governmental organization that was "involved in the legitimate gathering of information of public interest with the intention of imparting that information to the public and thereby contributing to the public debate."[84]

In October 2013, the Inter-American Commission on Human Rights held hearings on the impact of US surveillance on the freedom of expression.[85] However, it appears that the IACtHR has not yet issued any rulings concerning the impact of surveillance on this right, although (like the ECtHR) it has asserted that "[f]reedom of expression is an essential element of the freedom of the press."[86]

F. The right to a remedy

Finally, each of the human-rights treaties described in this paper mandates that States parties guarantee an effective remedy for any violation of the human rights enumerated in the texts.

1. The text of the relevant documents

Article 13 of the ECHR is the simplest of these provisions, and states that "[e]veryone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

---

[81] Weber v. Germany, *supra* note 9, paras. 143-146.

[82] *Id.,* paras. 147-149; see also Sunday Times v. the United Kingdom (No. 1), App. No. 6538/74, Judgment (Plenary), 2 Eur. H. R. Rep. 245 (1979).

[83] Weber v. Germany, *supra* note 9, paras. 147-153.

[84] Youth Initiative for Human Rights v. Serbia, App. No. 48135/06, Judgment, 2013 Eur. Ct. H. R. 584, paras. 6, 22-26.

[85] American Civil Liberties Union, IACHR Hearing on Freedom of Expression and Communications Surveillance by the United States, https://www.aclu.org/national-security/iachr-hearing-freedom-expression-and-communications-surveillance-united-states (last accessed June 26, 2014).

[86] Donoso v. Panama, *supra* note 74, ¶ 114.

Article 2(3) of the ICCPR contains a nearly identical provision, and further requires that a claim for a remedy be "determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State." It also requires states to "develop the possibilities of judicial remedy" and "ensure that the competent authorities shall enforce such remedies" when they are granted.

Meanwhile, Article 25 of the ACHR contains most of the same requirements as Article 2 of the ICCPR, although its text suggests that it may be applicable to violations committed by private actors as well as public authorities.

Article 18 of the American Declaration provides for remedies in rather different terms, mentioning only judicial remedies:

Every person may resort to the courts to ensure respect for his legal rights. There should likewise be available to him a simple, brief procedure whereby the courts will protect him from acts of authority that, to his prejudice, violate any fundamental constitutional rights.

2. Jurisprudence

The ECtHR has found that in order for a State to comply with the right to a remedy where violations of the rights guaranteed in the Convention are concerned, it is not always strictly necessary for an individual to be able to seek redress from a judicial forum.[87] However, especially when the available remedy is not judicial, a state must take care to ensure that the process for seeking redress is effective (as the text of Article 13 of the ECHR requires) as well as independent, in the sense of avoiding of a risk of undue influence by any of the authorities that allegedly were involved in the abuse.[88] Where a complaint stems from a surveillance program, "an effective remedy" under the ECHR means "a remedy that is as effective as can be, having regard to the restricted scope for recourse inherent in any system of secret surveillance for the protection of national security."[89] The Court stated in *Rotaru v. Romania* that "where secret surveillance is concerned, objective supervisory machinery may be sufficient" to meet the requirement for a remedy while the surveillance measures remain secret; "[i]t is only once the measures have been divulged that legal remedies must become available to the individual."[90] In a more recent case, however, the Court appeared to move away from this stance and toward a requirement for some kind of remedy—if only a "limited" one—even before the surveillance measures are completely declassified:

It is obvious that when surveillance is ordered and while it is under way, no notification of the persons concerned is possible, as such notification would jeopardise the surveillance's effectiveness. They are therefore of necessity deprived of the possibility to challenge specific measures ordered or implemented against them. However, this does not mean that it is altogether impossible to provide a limited remedy – for instance, one where the proceedings are secret and where no reasons are given, and the persons concerned are not apprised whether they have in fact been monitored – even at this stage.[91]

---

[87] Leander v. Sweden, *supra* note 32, para. 77.

[88] *Id.*; P.G. v. the United Kingdom, *supra* note 47, paras. 87-88.

[89] Klass v. Germany, *supra* note 25, para. 69.

[90] Rotaru v. Romania, *supra* note 30, para. 69.

[91] Ass'n for Eur. Integration and Human Rights v. Bulgaria, *supra* note 35, para. 100.

In any event, the remedy must still be such as to allow the competent authority "both to deal with the substance of the relevant … complaint [of a violation] and to grant appropriate relief."[92] The Court's jurisprudence implies that the grant of relief must be enforceable.[93]

At present, the IACtHR's findings in these respects appear to be restricted to its confirmation in *Tristan Donoso v. Panama* that states have a duty to undertake a diligent investigation of accusations of unlawful surveillance.[94]

IV. Conclusion

As the foregoing discussion shows, no state that engages in the clandestine surveillance of communications operates in an international legal vacuum: at minimum, it will be subject to the strictures of customary international law, particularly the binding norms pertaining to territorial and political integrity. The ways in which these norms constrain surveillance merit greater scrutiny by national and international courts as well as governments, UN bodies, and civil society.

Meanwhile, international human-rights courts, especially (but not solely) the ECtHR, have developed a detailed body of case-law concerning the legality of surveillance activities under international human-rights treaties. Although nearly all of these cases have concerned surveillance that took place within a state's own borders, and notwithstanding the many questions that continue to surround the extraterritorial applicability of a state's human-rights obligations, this jurisprudence is capable of providing very thorough guidance to states regarding whether their surveillance programs ensure that all persons enjoy fundamental rights at an adequate level. A substantial number of states—particularly in Europe—are bound at least internally by the judgments that have already been rendered, and it is incumbent upon the relevant courts to begin to clarify when a foreign individual (or locality) falls within a state's jurisdiction for the purposes of human-rights obligations where surveillance activities are concerned.

While much of the human-rights courts' existing case-law focuses on the right to privacy, the rights to freedom of expression and to an effective remedy for violations are also of paramount importance in this context, and the right to a remedy is particularly deserving of greater attention.

V. Glossary of Acronyms

ACHR: American Convention on Human Rights

CIL: Customary international law

---

[92] P.G. v. the United Kingdom, *supra* note 47, para. 85; *see also* Silver v. the United Kingdom, *supra* note 25, para. 116.

[93] *See* Silver v. the United Kingdom, *supra* note 25, para. 115.

[94] Donoso v. Panama, *supra* note 74, para. 146.

ECHR: European Convention on Human Rights

ECtHR: European Court of Human Rights

IACtHR: Inter-American Court of Human Rights

ICCPR: International Covenant on Civil and Political Rights

ICJ: International Court of Justice