Big Brother Watch and others v. the United Kingdom

Application no. 58170/13

WRITTEN SUBMISSIONS ON BEHALF OF THE INTERNATIONAL COMMISSION OF JURISTS (ICJ)

INTERVENER

pursuant to the First Chamber Registrar's notification dated 15 December 2015 that the President of the Chamber had granted permission under Rule 44 § 3 of the Rules of the European Court of Human Rights

---

9 February 2016

1. Introduction

In these submissions, the ICJ addresses (1) the scope of the right to privacy within the meaning of articles 8 ECHR and of their limitations in relation to metadata; (2) the attribution of State responsibility under international law for Convention violations caused via mass or 'bulk' surveillance programmes, in particular those involving the gathering of metadata and the related positive obligations of states, and (3) the application of the Convention to the extra-territorial dimensions of mass surveillance programmes on the enjoyment of this right. The present submissions reproduce *mutatis mutandis* the ICJ's submission in the case *Bureau of Investigative Journalism and Alice Ross v. United Kingdom.*

2. The right to privacy and information data (metadata)

In its jurisprudence, this Court has repeatedly held that the interception of communications engages article 8 ECHR.[1] It has further held that "[t]he mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8" and that "[t]he subsequent use of the stored information has no bearing on that finding."[2] The Court has not considered the nature of the content of the information significant for these purposes.[3]

The technical term "metadata" describes data that provides information about other data.[4] A typical manifestation of metadata has been described by the Court of Justice of the European Union (CJEU) as

> *"[including] data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of communication, to identify the 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 phone number, the number called and an IP address for Internet services. [They make it possible] 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."*[5]

Metadata allow for the drawing of very precise inferences as regards the private lives of the persons whose data has been intercepted, "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."[6] The Article 29 Working Party, an EU group gathering the authorities responsible for overseeing data protection in EU Member States, has affirmed that "metadata often yield information more easily

---

[1] *Malone v. United Kingdom,* ECtHR, Application No. 8691/79, Judgment of 2 August 1984, para. 64; *Weber and Saravia v. Germany,* ECtHR, Application No. 54934/00, Judgment (Admissibility) of 29 June 2006, para. 77; *Liberty and Others v. United Kingdom,* ECtHR, Application No. 58243/00, Judgment of 1 July 2008, para. 56; *Kennedy v. United Kingdom*, ECtHR, Application No. 26839/05, Judgment of 18 May 2010, para. 118; Article 8 ECHR is analogous to article 17 ICCPR.

[2] *S. and Marper v. United Kingdom*, ECtHR, Applications Nos. 30562/04 and 30566/04, Judgment [GC] of 4 December 2008, para. 67; *Leander v. Sweden*, ECtHR, Application No. 9248/81, Judgment of 26 March 1987, para. 48; *Amann v. Switzerland*, ECtHR, Application No. 27798/95, Judgment [GC] of 16 February 2000, para. 69.

[3] *Amann v. Switzerland*, op.cit., para. 70; *Digital Rights Ireland v. Minister of Communications & Others*, CJEU, cases C-293/12 and C-594/12, Judgment of 8 April 2014, para. 33.

[4] http://www.merriam-webster.com/dictionary/metadata (Accessd 29 January 2016).

[5] Digital Rights Ireland v. Minister for Communications & Others, op. cit., para. 26.

[6] *Ibid.*, para. 27.

than the actual contents of our communications do."[7] It also stressed that, both under the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention no. 108') and the EU Directive 95/46/EC, "metadata are personal data and should be protected."[8] The Venice Commission reached the same conclusion.[9]

Recent technological advances have significantly increased the capacity for sophisticated and invasive mass surveillance through gathering of communications data of email, mobile phone and internet services and have allowed a detailed profile of any individual's activities and relationships to be built using such intercepted data. As a result, this level of interception and surveillance has meant that the risk of infringement with the rights to private life has considerably grown.[10] In *Szabó and Vissy v. Hungary*, the Court stressed that "… the possibility occurring on the side of Governments to acquire a detailed profile … of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. …This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices."[11]

Article 8.2 ECHR envisages strictly limited circumstances that make some limitations permissible, where they are 'necessary in a democratic society' for the stated legitimate purposes. In relation to mass surveillance, including through interception and storage of metadata, the requirement of necessity in a democratic society means that the surveillance must be strictly necessary both for the interests enumerated in article 8 ECHR in general and for the obtaining of vital intelligence in an individual operation in particular. The Court has stressed that "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."[12]

The CJEU, in its recent *Schrems* judgment, held that legislation authorizing mass exchange of data, including metadata from the EU to the US, will not be considered strictly necessary "where it authorizes, on a generalized basis, storage of all the personal data of all the persons whose data has been transferred … without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail."[13] There is an even greater need for safeguards where personal data are undergoing automatic processing, especially when such data are used for police purposes.[14]

The UN High Commissioner for Human Rights, in a general report on *Human Rights in the Digital Age*, concluded that mass surveillance programmes are arbitrary *per se*.[15] Similarly, the Article 29 Working Party affirmed that "[u]nder no circumstances

[7] Article 29 Data Protection Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, EU Doc. 819/14/EN WP 215, 10 April 2014, p. 5.
[8] *Ibid*.
[9] European Commission for Democracy through Law (Venice Commission), *Report on the Democratic Oversight of Signals Intelligence Agencies*, adopted at its 102nd Plenary Session (Venice, 20-21 March 2015), Strasbourg, 15 December 2015 CDL-AD(2015)011, Study No. 719/2013, paras. 58-59.
[10] *Copland v. United Kingdom*, ECtHR, Application No. 62617/00, Judgment of 3 April 2007, para. 41; *Szabó and Vissy v. Hungary,* ECtHR, Application No. 37138/14, Judgment of 16 January 2016, para. 49.; Statement of the Article 29 Data Protection Working Party on the impact of the development of big data in the protection of individuals with regard to the processing of their personal data in the EU, adopted on 16 September 2014.
[11] *Szabó and Vissy v. Hungary*, op. cit., para. 70.
[12] *Ibid*., para 73.
[13] *Maximilan Schrems v. Data Protection Commissioner*, CJEU, case C-362/14, Judgment of 6 October 2015, para. 93.
[14] Digital Rights Ireland v. Minister of Communications & Others, op.cit., paras. 54-55.
[15] Report of the Office of the United Nations High Commissioner for Human Rights (OHCHR), *The right to privacy in the digital age*, UN Doc. A/HRC/27/37, paras. 25-26.

surveillance programmes based on indiscriminate, blanket collection of personal data can meet the requirements of necessity and proportionality."[16]

In light of the scale and scope of the interference with privacy entailed in mass surveillance, the ICJ submits that the distinction between acquisition of metadata and content surveillance is outdated and can no longer stand.

3. Mass surveillance programmes and State responsibility

The ICJ submits that any Contracting Party's responsibility under the Convention for co-operation in mass surveillance programmes must be circumscribed by the principles contained in the Articles on State Responsibility[17] of the International Law Commission ("ILC Articles"), which reflect customary international law.[18] There are several ways in which the involvement in a mass surveillance programme may engage the responsibility of a State under international law. First, the State initiating and administering the mass surveillance programme would typically be responsible for wrongful conduct, i.e. of human rights violations arising from this programme. Secondly, the international responsibility of a State may arise in case of cooperation or contribution, in the form of aid and assistance, to the mass surveillance programme.

3.1. Cooperation in a mass surveillance programme/system/enterprise

According to article 15 of the ILC Articles, a provision relied on by this Court in *El Masri*, a breach of international law may arise from "a series of actions or omissions defined in aggregate as wrongful",[19] i.e. a 'composite act'.[20] The ILC has equated this to the ECHR doctrine of 'practice incompatible with the Convention', defined as "an accumulation of identical or analogous breaches which are sufficiently numerous and inter-connected to amount not merely to isolated incidents or exceptions but to a pattern or system."[21]

The ICJ submits that certain mass surveillance programmes, such as those led by the US, through its National Security Agency, and its partner States, may constitute such a composite act or a 'practice incompatible with the Convention'. In mass surveillance programmes, the indiscriminate collection of data without effective safeguards and venues for redress has the potential to give rise to breaches of several Convention rights, including the right to privacy, that are 'sufficiently numerous and inter-connected' and that certainly do not amount to 'isolated incidents or exception', but rather to a true system of wrongful conduct. For example, the Parliamentary Assembly of the Council of Europe,[22] the UN High Commissioner for Human Rights,[23] and the European Parliament[24] have found that the current mass surveillance practices led by the US National Security Agency are based on the cooperation, at the very least, of the so-called "Five Eyes" (Australia,

---

[16] Article 29 Data Protection Working Party (10 April 2014), *op. cit.,* p. 6.
[17] International Law Commission (ILC), *Articles on the Responsibility of States for Internationally Wrongful Acts*, UN Doc. A/56/10, including commentaries contained therein: http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf; the articles were relied on by this Court in *Ilaşcu and others v. Moldova and Russia*, ECtHR, Application No. 48787/99, Judgment [GC] of 8 July 2004, paras. 320-321; and in *Verein gegen Tierfabriken Schweiz (VgT) v. Switzerland* (No.2), ECtHR, Application No. 32772/02, Judgment of 30 June 2009, para 86.
[18] *Case concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina v. Serbia and Montenegro*), International Court of Justice, Judgment of 26 February 2007, para. 420.
[19] ILC Articles, Article 15 para. 1.
[20] ILC Commentary, *op. cit.*, p. 62, Article 15, para. 2. "While composite acts are made up of a series of actions and omissions defined in aggregate as wrongful, this does not exclude the possibility that every single act in the series could be wrongful in accordance with another obligation"; *Ibid.*, p. 63, Article 15, para. 9.
[21] *Ireland v. United Kingdom*, ECtHR, Application No. 5310/71, Judgment of 18 January 1978, para. 159: "a practice does not of itself constitute a violation separate from such breaches."
[22] Parliamentary Assembly of the Council of Europe (PACE), *Resolution 2045 (2015)*, Mass surveillance A*ssembly debate*, 21 April 2015 (12th Sitting), para. 10.
[23] OHCHR Report, *op. cit.,* para. 4.
[24] European Parliament resolution of 12 March 2014, *op. cit.*, para. 1- 2.

Canada, New Zealand, the United Kingdom and the United States) and are used to "circumvent national restrictions by exchanging data on each other's citizens."[25] The Venice Commission, in a recent report, has highlighted the organized nature of the cooperation in these kind of operations:

> *"while many states co-operate with each other by exchanging domestic and foreign intelligence with one another (and such arrangements can also be part of a treaty obligation), the links between allied states as regards signals intelligence can be even stronger. Some states have standing co-operative arrangements and tight organisational links between their signals intelligence agencies."*[26]

The ILC commentaries affirm that "internationally wrongful conduct often results from the collaboration of several States rather than one State acting alone."[27] In this regard, the ILC refers to the case of *Certain Phosphate Lands in Nauru*, in which the International Court of Justice ruled that Australia could be held responsible for the actions taken by the Administering Authority for the Trust Territory of Nauru, which it jointly governed with the United Kingdom and New Zealand, not parties to the case before the Court.[28]

The ICJ submits that the mass surveillance programmes identified by the above-mentioned resolutions involve Contracting Parties and non-Contracting Parties, acting in organized and structured forms of cooperation. The organized and structured nature of their cooperation means that the States contributing to the 'composite act' or the 'practice' with the constructive knowledge of its capacity to cause multiple human rights breaches, may be held responsible for the internationally wrongful acts committed by and via this cooperation.

3.2. Contribution or assistance in the mass surveillance programme

The ICJ considers that, even outside of cases of organized and structured cooperation, States are also responsible where they aid or assist unlawful mass surveillance programmes that have the capacity to breach human rights obligations.

Article 16 of the ILC Articles establishes that "[a] State which aids or assists another State in the commission of an internationally wrongful act by the latter is internationally responsible for doing so if: (a) that State does so with knowledge of the circumstances of the internationally wrongful act; and (b) the act would be internationally wrongful if committed by that State."[29] State responsibility may arise either from positive steps taken to assist another State in a wrongful act, or from failure to take action, required by international legal obligations, that would have prevented a wrongful act by another State.[30] Consistent with these principles, the Convention imposes responsibility on States for both acts and omissions that entail co-operation in acts contrary to the Convention.

In *El-Masri,* this Court's Grand Chamber found that the responsibility of the Macedonian authorities was engaged throughout the whole period of an enforced disappearance, including the unacknowledged and secret detention of the applicant

[25] PACE, *op. cit.*, para. 10
[26] European Commission for Democracy through Law (Venice Commission), *op. cit*.
[27] ILC Commentaries, *op. cit.*, p. 64, Chapter IV, para. 2.
[28] *Case concerning Certain Phosphate Lands in Nauru (Nauru v. Australia)*, International Court of Justice, Preliminary Objections, Judgment of 26 June 1992, para. 48; ILC Commentaries, *op. cit.,* p. 64, Chapter IV, para. 2-3.
[29] ILC Articles on State Responsibility, Article 16; See further Commentary to Draft Article 16, *op. cit.,* paras.1- 6.
[30] ILC Commentaries, op. cit., Chapter IV, para. 4: "a State may be required by its own international obligations to prevent certain conduct by another State, or at least to prevent the harm that would flow from such conduct."; See also *Corfu Channel Case (United Kingdom of Great Britain and Northern Ireland v. Albania)*, International Court of Justice, Judgment of 9 April 1949, para. 22.

in Afghanistan, because of their active facilitation of the operation.[31] In *Al-Nashiri* and *Abu Zubaydah*, the Court found that Poland was internationally responsible for the violations that occurred during the rendition of the applicants, both within and outside its jurisdiction, "on account of its 'acquiescence and connivance' [and that], for all practical purposes, facilitated the whole process, created the conditions for it to happen and made no attempt to prevent it from occurring."[32] This was the case both for the victims' transfer to and from Poland.[33] The jurisprudence of the Court in these rendition operations led by the United States makes clear that States providing aid and assistance in the commission of a human rights violation need not be subject to the same treaty obligations as the main wrongful actor, but only to an equivalent obligation under international law. Such obligations may, for example, arise from different treaties, such as the European Convention on Human Rights and the International Covenant on Civil and Political Rights. The critical element for the purposes of State responsibility is that in respect of either State, the conduct is similarly proscribed and constitutes a wrongful act under international law.

These principles have been applied by the European Parliament, in the conclusions of its inquiry into the US-led surveillance system, to mass or 'bulk' surveillance programmes, when it affirmed "the transfer of personal data … in the absence of adequate safeguards and protections for the … fundamental rights of EU citizens, in particular the rights to privacy and the protection of personal data, would make that … Member State liable [for] any violation of the fundamental rights … ."[34]

In *Szabó and Vissy v. Hungary*, this Court has pointed out that "governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance … is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."[35]

The ICJ submits that - in accordance with article 16 of the ILC Articles - the responsibility of States that assist in mass surveillance programmes can be established from the point where those States had actual or constructive knowledge of the breaches of international human rights obligations inherent in that programme; and where the action of the Contracting Party contributed to the system.

3.3. Positive obligations of prevention in respect of mass surveillance

Under the positive obligations doctrine,[36] States must take measures to prevent action by third parties leading to violations of Convention rights. A State's positive obligation of prevention will be breached where it "knew or ought to have known" that the individual in question was at real and immediate risk of violation of his or her Convention rights, and failed to take reasonable measures of protection.[37] While such obligations must not "impose an impossible or disproportionate burden on the

[31] *El-Masri v. The Former Yugoslav Republic of Macedonia*, ECtHR, Application No. 39630/09, Judgment of 13 December 2012, para. 239.
[32] *Al-Nashiri v. Poland,* ECtHR, Application No. 28761/11, Judgment of 24 July 2014, para. 517; *Husayn (Abu Zubaydah) v. Poland*, ECtHR, Application No. 7511/13, Judgment of 24 July 2014, para. 512.
[33] *Al-Nashiri v. Poland,* op. cit*.,* paras. 517-518, and 539.
[34] European Parliament resolution of 12 March 2014, *op. cit.*, para. AD.
[35] Szabó and Vissy v. Hungary, op. cit., para. 78.
[36] *Osman v. United Kingdom,* ECtHR, Application No. 23452/94, Judgment [GC] 28 October 1998; *X and Y v. the Netherlands*, ECtHR, Application No. 8978/80, Judgment of 26 March 1985; *Kaya v. Turkey*, ECtHR, Application No. 22535/93, Judgment of 28 March 2000; *Storck v. Germany*, ECtHR, Application No.61603/00, Judgment of 16 June 2005; *Costello-Roberts v. United Kingdom*, ECtHR, Application No. 13134/87, Judgment of 25 March 1993; *Hatton v. United Kingdom*, ECtHR, Application No. 36022/97, Judgment [GC] of 8 July 2003; *Keenan v. United Kingdom,* Application No. 27229/95, Judgment of 3 April 2001. See also the *Reply by the Committee of Ministers to Parliamentary Assembly Recommendation 1801 (2007) on Secret detentions and illegal transfers of detainees involving Council of Europe member states*, Doc. 11493 (19 January 2008), adopted at the 1015th meeting of the Ministers' Deputies on 16 January 2008, para. 3.
[37] *Osman v. United Kingdom*, op. cit., para. 116.

authorities", the latter must do "all that could be reasonably expected of them"[38] to prevent violations and end those that are ongoing.

The fact that, in a mass surveillance operation, elements of the violation(s) of rights typically take place outside the jurisdiction of the State where the affected individual is physically present, does not preclude the responsibility of that State. In *Rantsev v. Cyprus and Russia*, the Court held that it was within its competence to consider Russia's responsibility for violations of the rights of a victim of trafficking, transferred by private actors from Russia to Cyprus, despite the fact that the majority of the violations of the victim's rights took place outside Russia.[39] This was related to the nature of the criminal enterprise giving rise to the human rights abuses: cross-border trafficking that "may take place in the country of origin as well as in the country of destination."[40] This doctrine was also applied in *Al-Nashiri* and *Abu Zubaydah*, cases of complicity in the US-led rendition programme, where the Court found that, "Poland was required to take measures designed to ensure that individuals within its jurisdiction were not subject to"[41] violations of the victims' Convention rights.

The UN Human Rights Committee has stated, in relation to ICCPR rights, that States have positive obligations to take effective measures 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."[42] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has affirmed the same obligation: "to protect those affected against misuse by State organs as well as private parties"[43]

In fulfillment of their positive obligations,[44] the European Parliament has called on EU Member States "to refrain from accepting data from third states which have been collected unlawfully and from allowing surveillance activities on their territory by third states' governments or agencies which are unlawful under national law or do not meet the legal safeguards enshrined in international or EU instruments, including … the ECHR … ."[45] It has particularly stressed the duty not to share or receive intelligence data that could cause or would originate from human rights violations.[46]

The Committee of Ministers of the Council of Europe has called on Member States to bear in mind risks for privacy caused by digital tracking and other surveillance technologies "in their bilateral discussions with third countries."[47] In 1991, it had recommended that "communication, in particular by electronic means, of personal data or personal data files by public bodies to third parties should be accompanied by safeguards and guarantees designed to ensure that the privacy of the data subject is not unduly prejudiced." [48] Further guidance is contained in other

[38] *Ibid.*, paras. 115-116. These positive obligations are reflected elsewhere in international human rights law, including under the ICCPR (Article 2 ICCPR. UN CCPR, GC 31, para.8) and the Convention against Torture (Article 2 UNCAT).
[39] *Rantsev v. Cyprus and Russia*, ECtHR, Application No. 25965/04, Judgment of 7 January 2010, paras. 207-208.
[40] Ibid., para. 307.
[41] Al-Nashiri v. Poland, op. cit., para. 517; Husayn (Abu Zubaydah) v. Poland, op. cit., para. 512.
[42] Human Rights Committee, *General Comment 16*, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994), para 10.
[43] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/17/27, 16 May 2011, para. 58
[44] European Parliament resolution of 12 March 2014, *op. cit.*, para. 27
[45] *Ibid.*, para. 25.
[46] European Parliament resolution of 8 September 2015 on '*Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries*' (2014/2232(INI)), para. 4.
[47] *Declaration of the Committee of Ministers on* 11 June 2013, op. cit., para. 8.
[48] Recommendation no. R(91)10 of the Committee of Ministers to Member States on the Communication to Third Parties of Personal Data held by Public Bodies, adopted by the Committee of Ministers on 9 September 1991 at the 461st meeting of the Ministers' Deputies, Appendix, para. 2.1.

documents of the Committee of Ministers.[49] The Article 29 Working Party has affirmed, with regard to the introduction of automated data exchange systems among countries for tax purposes, that this "implies bigger (security) risks and liability under EU data protection laws. Therefore, such model … has to be complemented by adequate measures to respond to the increased risks and responsibilities."[50]

The ICJ submits that the positive obligations of States under article 8 ECHR with regard to data transfer should be read in light of other sources of international law binding upon Contracting Parties.[51] Convention no. 108[52] and the *Recommendation on the Communication to Third Parties of Personal Data held by Public Bodies* require that, to allow for the free flow of transborder communications, the system of privacy rights protection in third countries to which data is transferred must be adequate in comparison to that of the Contracting Party from which the data is sent (principle of adequacy of protection systems).[53] More recently, an Additional Protocol to Convention no. 108 obliges States to "provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer."[54] The European Parliament, in its conclusion to its mass surveillance inquiry, also called on EU Member States to respect the principle of adequate privacy rights protection in transfer of data to third countries, as did the CJEU in the *Schrems* case in relation to EU Directive 95/46/EC.[55]

The ICJ submits that, under international law, in mass surveillance programmes whereby a State establishes a system of interception, storage and intelligence cooperation in the field of surveillance and data transfer, or has participated or contributed to a mass surveillance programme, or knows or ought to have known of such a mass surveillance programme, the State has the obligation to establish an appropriate system of safeguards in relation to the programme for the respect and protection of the right to privacy under articles 8 of the Convention.

In addition, States Parties to the ECHR and Convention no. 108 have a duty to take steps to protect the right to privacy of the persons subject to their jurisdiction from the violations of article 8 ECHR rights caused by mass surveillance programmes. In particular, in light of the obligations under Convention no. 108, they should ascertain that an adequate level of protection of these rights exists in countries where data is to be transferred.

[49] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, a*dopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies* (the UK reserved its position on this Recommendation), paras. 2.2, 6, and 8.1.

[50] Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes (14/EN WP 230), adopted on 4 February 2015, para 2.

[51] *Al-Adsani v. the United Kingdom,* ECtHR, Application No. 35763/97, Judgment [GC] of 21 November 2001*,* para. 55.

[52] Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data ('Convention No. 108')*, 28 January 1981, entry into force 1 October 1985, ETS 108, preamble and article 1.

[53] Convention No. 108, Article 12.3.a; Recommendation no. R(91)10 of the Committee of Ministers, *op. cit.,* Appendix, 8.3-8.4.

[54] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, CETS Np.181, Article 2.1. While this Additional Protocol has not been ratified by all Council of Europe Members, the eight signatory countries, have the obligation to refrain to act against its object and purpose under article 18 of the Vienna Convention on the Law of Treaties 1969. As explained in its Preamble, the object and purpose of the Additional Protocol is "to ensure the effective protection of human rights and fundamental freedoms, and in particular the right to privacy, in relation to such exchanges of personal data."

[55] European Parliament resolution of 12 March 2014, *op. cit.,* para. 41

4. The extraterritorial dimensions of the right to privacy applied to surveillance activity

Given the transborder nature of internet communication, the obligations of States (both negative and positive) in regard to mass interception of internet data necessarily apply extraterritorially in certain situations. As discussed in the previous section, States have obligations under the Convention to respect and to take positive measures to protect privacy rights in respect of persons on their territory. However, a State may also be responsible under the Convention for the interception of data originating from outside its jurisdiction where it operates or contributes to (see section 2 above) a mass surveillance programme.

In *Weber and Saravia v. Germany*, the Court held that "the transmission of data to and their use by other authorities, which enlarged the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned,"[56] would be an interference with the right to privacy under article 8 ECHR. The Court found in that case that Germany would be responsible for violations of the right to privacy of persons located outside of Germany via interception of satellite or radio signals from facilities located in Germany.[57]

Notably, Convention no. 108 does not apply the principle of adequacy of protection to a State in relation to data that is imported into the State as this "presents no problems because imported data are in any case covered by the data protection regime of the importing State."[58] Consequently, a State that imports information from a third State or that intercepts information coming from a third State would be responsible for human rights violations occurring on its territory caused by such interception. The ICJ further notes that Convention no. 108 mandates that States "assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this Convention".[59] The Convention recognizes the fact that the State of location of the entity with control over the information/data is under an obligation to provide protection and redress for the right's violations. The Committee of Ministers of the Council of Europe has held that, in the context of the internet, "states should … refrain from any action that would directly or indirectly harm persons or entities outside of their territorial jurisdiction."[60]

Therefore, in cases of mass surveillance, the State's authority or control over the information, and therefore of an important element of the private sphere of the person concerned, is sufficient to establish jurisdiction, irrespective of the location of the individual concerned. This reflects the general principles of jurisdiction established by the Court, which has repeatedly affirmed, notably in *Al-Skeini and others v. United Kingdom,* that, "a Contracting State's jurisdiction under Article 1 may extend to acts of its authorities which produce effects outside its own territory."[61] In particular, the Court has held that such jurisdiction may arise either "when, through the consent, invitation or acquiescence of the Government of that territory, it exercises all or some of the public powers normally to be exercised by that Government" on the territory or in situations where a Contracting party, in the absence of territorial control, nevertheless "exercises control and authority over an individual"[62]

[56] *Weber and Saravia v. Germany*, op. cit., para. 79.
[57] Ibid., para. 88.
[58] Explanatory Report to Convention no. 108, para. 66.
[59] Convention No. 108, Article 14.1.
[60] Declaration by the Committee of Ministers on Internet governance principles, adopted by the Committee of Ministers on 21 September 2011 at the 1121st meeting of the Ministers' Deputies, para 3.
[61] *Al-Skeini and Others v. United Kingdom*, ECtHR, Application No. 55721/07, Judgment [GC] of 7 July 2011, para.133
[62] Ibid., para.137

In this regard, the UN High Commissioner for Human Rights has recalled that, under international human rights law,

> "digital surveillance … may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found … . 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 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."[63]

The UN Human Rights Committee stressed that, with respect to the applicability of the *International Covenant on Civil and Political Rights*, "it would be unconscionable to permit a state to perpetrate violations on foreign territory which violations it could not perpetrate on its own territory."[64] It has affirmed that the reference to 'jurisdiction' in the First Optional Protocol "is not to the place where the violation occurred, but rather to the relationship between the individual and the State in relation to a violation of any of the rights set forth in the Covenant, wherever they occurred."[65]

As recognized in the Court's jurisprudence on article 8 ECHR, privacy rights extend to aspects of the personal sphere of an individual, beyond their physical integrity. **The ICJ therefore submits that jurisdiction as regards mass surveillance should be interpreted such that, even where a State exercises authority and/or control over personal information of an individual physically outside the territory of the Contracting Party, the person should be recognised as coming within the authority and/or control of the State, for the purposes of rights that relate to such information, in particular rights under article 8 ECHR.**

[63] OHCHR Report, *op. cit.,* para. 34.
[64] *Sergio Euben Lopez Burgos v. Uruguay*, Human Rights Committee Communication No. R.12/52, UN Doc. Supp. No. 40 (A/36/40) at 176 (1981), para. 10.3.
[65] *Ibid.*, para. 12.2.