Eliza Watt
16.10.2016

THE RIGHT TO PRIVACY AND THE FUTURE OF MASS SURVEILLANCE

Introduction

Peacetime espionage is by no means a new phenomenon in international relations.[1] For as long as it has existed, it has been a prevalent method of gathering intelligence from afar, including through electronic means.[2] However, foreign cyber surveillance on the scale revealed by Edward Snowden performed by the United States National Security Agency (NSA), the United Kingdom Government Telecommunications Headquarters (GCHQ) and their Five Eyes partners[3] is a relatively recent activity. It can be defined as targeted and untargeted interception, bulk collection and storage of digital communications (content and metadata[4]). Foreign cyber surveillance comprises both transnational and extraterritorial surveillance.[5] It may be conducted through the use of a variety of tools and programmes, such as PRISM and Tempora. The latter, predominantly used by the UK intelligence services, allows accessing of global communications through tapping of the fibre-optic underwater cables, giving GCHQ the ability to monitor up to 600 million communications every day.[6]

---

[1] Geoffrey B. Demarest, 'Espionage in International Law' (1996) 24 Denver Journal of International Law and Policy 321, 326. Demarest defines espionage as 'the consciously deceitful collection of information, ordered by a government or organization hostile to or suspicious of those the information concerns, accomplished by humans authorised by the target to do the collecting'.

[2] Russell Buchan, 'The International Legal Regulation of State-Sponsored Cyber Espionage' in Anna Maria Osula and Henry Roigas (eds), *International Cyber Norms: Legal, Policy and Industry Perspective* (NATO CCD COE Publications, Tallinn 2016) 65-86.

[3] Privacy International, 'The Five Eyes' < https://www.privacyinternational.org/node/51> The Five Eyes alliance is a secretive, global surveillance arrangement of states comprised of the United States National Security Agency, the United Kingdom Government Communications Headquarters, Canada's Communications Security Establishment Canada, the Australian Signals Directorate and New Zealand's Government Communications Security Bureau.

[4] Privacy International, 'Metadata' < https://www.privacyinternational.org/node/53> Metadata is information about the communication and include, *inter alia*, the location that the communication derived from, the device that sent it, the time it was sent and information about the recipient.

[5] Ashley Deeks, 'An International Legal Framework for Surveillance' (2015) 55 Virginia Journal of International Law 292-367, 299-300. Transnational surveillance refers to the surveillance of communications that cross state borders, including those that begin and end overseas but incidentally pass through the collecting state. Extraterritorial surveillance refers to the surveillance of communications that take place entirely overseas.

[6] Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, 'Mass Surveillance. Who is Watching the Watchers?' (Doc 13734, 2015) 6.

NSA's PRISM enables direct access of the customer data from nine internet firms, including Google, Microsoft and Yahoo. [7]

This article examines the legality of foreign cyber surveillance of NSA and GCHQ from the perspective of international human rights law, specifically the right to privacy under Article 17 International Covenant of Civil and Political Rights 1966 (ICCPR)[8] and Article 8 European Convention on Human Rights 1950 (ECHR).[9] Since these activities are likely to continue, important questions regarding future protection of privacy of millions of people world-wide must be addressed both nationally and internationally. The United Nations (UN) and regional human rights bodies and organizations have voiced concerns, but these seem to fall on deaf ears. This article therefore explores the viability of a legally binding, multilateral cyber surveillance treaty to regulate the practices of intelligence gathering at home and abroad. Such a treaty, called the 'intelligence Codex' (the Codex), has recently been proposed by the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe (PACE).[10] It is a multilateral 'no-spy' regional instrument among European countries, which aims to lay down rules governing cooperation for purposes of the fight against terrorism and organized crime.[11] The idea has been put forward to the ministers of the 47 Council of Europe member states, but has already met with one rejection from the Netherlands. The Dutch government objected to the banning of economic and political espionage set out in the Codex, for being unrealistic and with a potential to 'irresponsibly limit intelligence collection'.[12]

---

[7] ibid.

[8] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 17 provides

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

[9] Convention for the Protection of Human Rights and Fundamental Freedoms (opened for signature 4 November 1950, entered into force 3 September 1953) 213 UNTS 222 (ECHR), art 8 provides:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be on interference by a public authority with the exercise of this right except such as 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.

[10] supra note 6, Parliamentary Assembly of the Council of Europe Resolution 2045 (21 April 2015).

[11] ibid, para 17.4.

[12] Matthijs Koot, 'Dutch Government Rejects Idea of No-Spy Agreements Between European Countries' (13 March 2015)< https://blog.cyberwar.nl/2015/03/dutch-minister-of-the-

This article takes a different view and considers the Codex as a step in the right direction. The issuing discussion is divided into five sections. Section one outlines the domestic legal bases authorising foreign cyber surveillance and demonstrates that they unjustly discriminate on the basis of nationality. Section two makes a case for the extraterritorial application of human rights treaties in the context of cyber surveillance abroad. Section three shows how cyber surveillance amounts to an interference with the right to privacy of communications and section four finds no justifications for the interference, as set out in Article 17 ICCPR and Article 8(2) ECHR. This leads to the inevitable conclusion in section five that foreign cyber surveillance should no longer be permitted to operate in an international regulatory legal vacuum. To that end, this section supports the idea of a legally binding agreement as proposed by the Council of Europe.

1. Cyber Surveillance Programmes and Their Domestic Legal Bases

The activities of NSA and GCHQ are secretive by definition. However, the global condemnation of the US and the UK sponsored surveillance has caused the US government to admit the existence of PRISM. Whilst the UK confirmed that it has been the recipient of data from PRISM via its intelligence sharing relationship with the US,[13] the government has adopted a 'neither confirm nor deny' policy towards Tempora.[14]

PRISM operates pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA).[15] This provision was introduced by the FISA Amendment Act (FAA) 2008, which revised the previous surveillance rules. The FAA adopts different approaches depending on whether the targets of surveillance are 'United States persons',[16] or 'non-United States' persons[17] and may be summarised as follows: (a) US persons can be targeted only upon showing a probable cause to believing that he/she is an agent of a foreign power, [18] whereas non-US persons can be targeted showing a lower 'reasonable belief' standard; (b) US persons may only be targeted if there is a judicial warrant from the Foreign Intelligence Surveillance Court (FISC), whereas non-US persons can be targeted without FISC approved individual

---

interior-rejects-eu-pace-proposal-omtzigt-of-anti-spy-treaty-between-european-countries/>.

[13] Liberty, 'Liberty's Evidence to the Intelligence and Security Committee's Inquiry into Privacy and Security' (February 2014) < https://www.liberty-human-rights.org.uk/sites/default/files/Liberty%20evidence%20to%20the%20ISC%20inquiry%20into%20privacy%20and%20security%20(Feb%202014).pdf>, 3.

[14] ibid.

[15] 50 U.S.C § 1881(a).

[16] 50 U.S.C § 1881(c). United States persons are defined as American citizens or non-citizens who are legal permanent residents in the US.

[17] 50 U.S.C § 1881(a).

[18] Richard A. Clarke et al, *The NSA Report. Liberty and Security in the Changing World. The President's Review Group on Intelligence and Communications Technologies* (Princeton University Press 2013) 86-87.

warrants; (c) the minimization requirements for communications of US persons would not extend fully to non-US persons located outside the US.[19]

The UK surveillance powers to intercept foreign communications are set out primarily in the Regulation of Investigatory Powers Act 2000 (RIPA), soon to be replaced by the Investigatory Powers Bill.[20] RIPA too makes a distinction, but between 'internal' and 'external' communications. 'Internal interceptions' may only be conducted on the basis of individual warrants,[21] which must name, or describe a person, or single set of premises to be intercepted.[22] Conversely, the interception of 'external communications',[23] i.e. 'means of communications sent or received outside the British Islands',[24] are very loosely controlled. A warrant does not need to identify a specific person, or premises but must only contain the description of intercepted material. There is no upper limit to the number of external communications that may be intercepted on the basis of s8(4) RIPA and warrants granted pursuant to this section can last for either three, or six months and be renewed indefinitely.

The discriminatory nature of s 702 FAA 2008 and s 8 RIPA 2000 is clear, but it is just a part of a wider US and its Five Eyes partners' policy stance post 11 September 2001, which places emphasis on citizenship as a basis for fundamental rights.[25] This therefore requires that the rights of non-citizens be clarified under international law. The fundamental recognition that all persons by virtue of their essential humanity are equal and should enjoy all human rights without discrimination is contained in Article 2(1) of the Universal Declaration of Human Rights;[26] Articles 2[27] and 26[28] of the ICCPR; Articles 1[29] and 2[30] of the International Covenant of on Economic Social and Cultural Rights 1976 (ICESCR); and Article 14[31] of the ECHR. The UN Human Rights Committee (HRC), a body of independent experts that monitors the implementation of the ICCPR by its state parties, is tasked with providing

---

[19] ibid.
[20] UK Parliament, 'Investigatory Powers Bill. Explanatory Notes' (18 May 2016) <http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0002/en/17002en03.htm>
[21] Regulation of Investigatory Powers Act 2000 s 5.
[22] RIPA 2000 s 8(1).
[23] RIPA 2000 s 8(4)-(6).
[24] RIPA 2000 s 20.
[25] Marko Milanovic, 'Foreign Surveillance and Human Rights, Part 1: Do Foreigners Deserve Privacy?' (EJIL: Talk! 25 November 2013) <http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-1-do-foreigners-deserve-privacy/>.
[26] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 2(1).
[27] ICCPR supra note 8, art 2(1).
[28] ICCPR supra note 8, art 26.
[29] International Covenant on Economic Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) UNTS 993 (ICESCR) art 1.
[30] ICESCR, ibid art 2.
[31] ECHR, supra note 9, art 14.

a guide to the Covenant's interpretation. This the Committee does through issuing non-country specific and non-legally binding general comments, with the purpose to, *inter alia*, promote the effective implementation of the Covenant, clarify its requirements and stimulate the activities of state parties as well as international organizations in the promotion and protection of human rights.[32] In General Comment No. 15 in relation to the rights under the ICCPR, the HRC explained that the rights in the Covenant apply to everyone, irrespective of their nationality and the general rule is that each one of these rights must be guaranteed without discrimination between citizens and aliens.[33] The ICESCR likewise established that governments shall take progressive measures to the extent of available resources to protect the rights of everyone regardless of their citizenship.[34] Thus, the fundamental principle dictates that human rights are presumptively owned to citizens and non-citizens alike, unless a particular treaty (or customary rule) allows for differential treatment. Both the ICCPR and the ICESCR permit states to draw distinctions between citizens and non-citizens, but only with respect to three categories of rights, namely political rights, freedom of movement and economic rights in developing countries.[35] Thus, under Article 25 ICCPR, the right to participate in public affairs, to vote, to hold office and to have access to public services is guaranteed to citizens only.[36] Similarly, Article 12(4) ICCPR provides that no one shall be arbitrarily deprived of the right to enter his own country, [37] whilst the ICESCR Article 2(3) allows developing counties to 'determine to what extent they would guarantee the economic rights recognized in the present Covenant to non-nationals'.[38] States therefore may not draw distinction between citizens and non-citizens as to social and cultural rights, with exception of the right to public participation and of movement. Having said that, international law, as well as state practice consistently sanctions discrimination and distinctions on the basis of nationality, which means some discrimination on these grounds would be permissible.[39] The HRC in its General Comment No. 18 clarified this by stating that 'not every differentiation of treatment will constitute discrimination, if the criteria for such a differentiation are reasonable and objective and if the aim is to achieve a purpose, which is legitimate under the [International] Covenant [of Civil and Political Rights]'[40] and is proportional to the achievement of that objective.[41] The 'objective and reasonable justification' is also a criteria that the European Court of Human Rights (ECtHR) requires a state to satisfy in order to show that the difference in treatment

---

[32] Ghandi, *The Human Rights Committee and the Right of Individual Communication: Law and Practice* (Ashgate Publishing 1998) 25.
[33] UNHRC, 'General Comment No. 15. The Position of Aliens under the Covenant' (1986) UN Doc HRI/Gen/1/Rev.9/(Vol.1) para 1-2.
[34] ICESCR, supra note 29 art 2.
[35] supra note 33 para 18.
[36] ICCPR, supra note 8 art 25.
[37] ICCPR, supra note 8 art 12(4).
[38] ICESCR, supra note 29 art 2(3).
[39] supra note 33 para 23-30.
[40] UNRC, 'General Comment No. 18: Non-Discrimination' (1989) UN Doc HRI/GEN/1/Rev.1 para 13.
[41] UNCHR (Sub-Commission), 'Report by Special Rapporteur David Weissbrodt 2003/23' (2003) UN Doc E/CN.4/Sub.2/2003/23.

was not discriminatory. In *Burden v United Kingdom*[42] the Strasbourg Court held that 'a difference of treatment is discriminatory if it has no objective and reasonable justification; in other words, if it does not pursue a legitimate aim and if there is not a reasonable relationship of proportionality between the means employed and the aim sought to be realised. The Contracting State enjoys a margin of appreciation in assessing whether and to what extent differences in otherwise similar situations justify a different treatment'.[43]

States are obliged to ensure that measures taken in the struggle against terrorism do not discriminate in purpose or effect on grounds of nationality and the principle of non-discrimination must be observed in all matters, in particular in those concerning liberty, security and dignity of the person, equality before the courts and due process of law, as well as international cooperation in judicial and police matters.[44] In guaranteeing certain rights to citizens only, the US and the UK laws breach the provisions of non-discrimination and equal treatment under the ICCPR and the ECHR, which as will be shown below cannot be justified on objective and reasonable grounds. Indeed, 'the unique position of the United States (and the United Kingdom) with regards to the physical infrastructure of the internet and the fact that the private companies based in the US collect and store huge amounts of data of persons residing anywhere in the world makes the exclusion of "non-US [and UK] persons" from any legal protection against mass surveillance simply intolerable-it may well lead to the destruction of the internet as we know it'.[45] This reinforces the need to broaden the scope of the extraterritorial application of these states' human rights obligations to apply to foreign cyber surveillance, discussed next.

2. Extraterritorial Application of the ICCPR and ECHR and Cyber Surveillance

Article 17 ICCPR and Article 8 ECHR apply extraterritorially, which means that states must respect the right to privacy whenever individuals are within their territory as well as their jurisdiction.[46] However, the US has long denied that it has obligations to respect and protect human rights outside its borders (territory), despite views to the contrary expressed by most international human rights courts and bodies.

The jurisdictional scope of application of the ECHR and the ICCPR are set out in Article 1[47] and Article 2(1)[48] respectively. The US has consistently held a narrow stance

---

[42] *Burden v United Kingdom* (App no 133378/05) (2008) ECHR 357 [GC].

[43] ibid, para 60.

[44] supra, note 41 para 28.

[45] Council of Europe Committee on Legal Affairs and Human Rights, 'Mass Surveillance-Report of the Parliamentary Assembly' (2015) Doc 13734 45.

[46] American Civil Liberties Union, 'Privacy Rights in the Digital Age. A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant of Civil and Political Rights: A Draft Report and General Comment by the American Civil Liberties Union' (2014) <https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf> 28.

[47] ECHR, supra note 9 art 1:

> 'The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.'

[48] ICCPR, supra note 8 art 2(1):

regarding extraterritorial application of the Covenant since its statement to the Human Rights Committee in 1995.[49] This position has been based on Article 31(1) of the Vienna Convention on the Law of the Treaties (VCLT), which requires that treaties should be read 'in accordance with the ordinary meaning …of [their] terms'. [50] The US approach is that obligations under the ICCPR will only arise if both conditions in Article 2(1) ICCPR are satisfied, that is an individual must be 'within its territory' *and* 'subject to its jurisdiction', which rules out the extraterritorial application of the ICCPR altogether. This interpretation, in particular in relation to foreign cyber surveillance, must be rejected in favour of the more expansive view taken by international bodies, according to which a state must ensure human rights within its territory and anywhere it has 'effective control' of either the territory, or a person. There are number of reasons for this. First, the narrow approach favoured by the US has been repeatedly criticized by the Human Rights Committee in its 1994,[51] 2006 and 2014 reports.[52] Secondly, the HRC endorsed the extraterritorial application of the Covenant, also relying on Article 31 VCLT, but unlike the US, the Committee invoked its 'object and purpose' to determine that the conditions contained in Article 2(1) ICCPR should not be determined conjunctively, but disjunctively. According to its General Comment No. 31, states must respect and ensure the rights laid down by the Covenant to

---

> Each 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, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

[49] UNHRC, 'Summary Record of the 1405th Meeting' (24 April 1995) UN Doc CCPR/C/SR/1405. The US Government's position was made clear in para 20:

> The Covenant was not regarded as having extraterritorial application (…) Article 2 of the Covenant expressly stated that each State party undertook to respect and ensure the rights recognized 'to all individuals within its territory and subject to its jurisdiction'. That dual requirement restricted the scope of the Covenant to persons under the United States jurisdiction and within United states territory.

[50] Vienna Convention on the Law of the Treaties (adopted 22 May 1969) (1969) 1155 UNTS 331 (VCLT) art 31(1).

[51] UNHRC, 'Report of the Human Rights Committee' (1995) UN Doc A/50/40 para 284:

> [the HRC] does not share the view [of the US government] that the Covenant lacks extraterritorial reach under all circumstances [because] such a view is contrary to the consistent interpretation of the Committee … that in special circumstances, persons may fall under the subject-matter jurisdiction of a State Party even when outside that State's territory.

[52] UNHRC, 'Concluding Observations on the US Report Under the ICCPR' (2006) UN Doc CCPR/C/USA/CO/3; UNHRC, 'Concluding Observations on the US Report Under the ICCPR' (2014) UN Doc CCPR/C/USA/CO/3. Both reports state in para C.4 that:

> The Committee regrets that the State Party continues to maintain its position that the Covenant does not apply with respect to individuals under its jurisdiction but outside its territory, despite the contrary interpretation of article 2(1) supported by the Committee's established jurisprudence, the jurisprudence of the International Court of Justice and State practice.

anyone within the power or effective control of that state party, even if not situated within its territory.[53] Additionally, the HRC considered that 'state parties are required to give effect to the obligations under the Covenant in good faith' pursuant to Article 26 of the VCLT.[54] The HRC adopted this expansive approach in several cases, such as Lo*pez Burgos v Uruguay,*[55] *Montego v Uruguay*[56] and in *Munaf v Romania.*[57] Recently, the HRC in its General Comment No. 35[58] concerning Article 9 ICCPR[59] confirmed that '[s]tate [p]arties have an obligation to respect and ensure the rights under Article 9 to all persons who may be within the territory and to all persons subject to their jurisdiction'.[60] When considering the US cyber surveillance activities in its 2014 report, the HRC clearly found that foreign surveillance implicates ICCPR, stating the the US should 'take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including Article 17.'[61] Thirdly, the established jurisprudence of other international courts, such as the International Court of Justice (ICJ) and the European Court of Human Rights also support the wider, extraterritorial application of human rights treaties. In the *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories* Advisory Opinion[62] and the *Case Concerning Armed Activities on the Territory of the Congo,*[63] the ICJ concluded that the ICCPR was applicable 'in respect to acts done by a State in the exercise of its jurisdiction outside its own territory'.[64] By far the most developed

---

[53] UNHRC, 'General Comment No. 31. The Nature of the General Legal Obligations Imposed on State Parties to the Covenant' (2004) UN Doc CCPR/C/21/Rev.1/Add.1326 May 2004.
[54] VCLT, supra note 50 art 26.
[55] *Lopez Burgos v Uruguay* (1979) UNHRC Communication No 52/1979 UN Doc CCPR/C/13/D/52/1979. The HRC held that state parties are liable for the actions of their agents on foreign territory and stated that states must respect and ensure the Covenant rights to all persons who may be within their territory or subject to their jurisdiction.
[56] *Montego v Uruguay* (1981) UNHRC Communication No 106/1981 UN Doc Supp No 40 (A 138/40). This case concerned a refusal of the Uruguay authorities to renew the passport of an Uruguay citizen residing in Germany. The Committee found that in the case of citizens residing abroad Article 2(1) cannot be interpreted as limiting the obligations of Uruguay under Article 12(2) (free movement) to citizens within its own territory.
[57] *Munaf v Romania* (2006) UNHRC Communication No 1539/06 UN Doc CCPR/C/96/D. The Committee observed that a state may be liable for human rights violations that occur even outside its area of control, as long as that state's activity was 'a link in a causal chain' bringing about the human rights violations.
[58] UNHRC, 'General Comment No. 35. Article 9-Liberty and Security of Person' (2014) UN Doc CCPR/C/GC/35.
[59] ICCPR, supra note 8 art 9.
[60] supra, note 58 para 63.
[61] UNHRC, 'Concluding Observations on the Fourth Periodic Report of the United States of America' (2014) UN Doc CCPR/C/USA/CO/4 para 22.
[62] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories* (Advisory Opinion) 2004 ICJ Reports 163.
[63] *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v Uganda)* (Request for the Indication for Provisional Measures: Order) [2000] ICJ Reports 111.

and varied jurisprudence on the issue of extraterritoriality however is that of the ECtHR interpreting Article 1 ECHR. The approach taken by the Strasbourg Court in *Al-Skeini v United Kingdom*[65] clarified its earlier stance on the issue.[66] The Court reaffirmed two basic models of state jurisdiction: the spatial model (jurisdiction as effective overall control by a state over an area, or territory)[67] and the personal model (jurisdiction as an exercise of authority, or control by state agents over an individual),[68] emphasising however that extraterritorial application of ECHR can only be exceptional and needs to be justified by reference to general international law.[69] Post *Al-Skeini* cases attest to a more expansive view towards the question of extraterritorial application of the Convention, with regards to both the personal (*Jaloud v the Netherlands*)[70] and the spatial model (the so-called *Nagorno-Karabakh* cases).[71] These cases are a clear indication of the trend in the ECtHR jurisprudence towards clearer, more factual and importantly more permissive approach,[72] which also is in line with other human rights bodies.[73]

Neither the HRC, nor the ECtHR has yet pronounced directly on the extraterritorial application of the ICCPR and ECHR to cases of cyber surveillance.[74] Nevertheless, they may

---

[64] supra, note 62 para 111; DRC v Congo, ibid.

[65] *Al-Skeini and Others v United Kingdom* (App No 55721/07) [2011] ECHR 1093.

[66] *Bankovic and Others v Belgium and Others* (App No 52207/99) [2001] ECHR 890. The case concerned the violation of the right to life of victims of the 1999 NATO aerial bombings in Kosovo. The ECtHR held that the jurisdictional competence of a state is primarily territorial, thus resisting the extraterritorial application of ECHR, allowing however for one exception, namely the inhabitants of a territory being under the effective control of an ECHR contracting party (para 80). See also *Ilaşcu and Others v Moldova and Russia* (App No 48787/99) (2005) 40 EHRR; *Loizidou v Turkey* (App No 15318/89) (1995) 23 EHRR 513; *Issa and Others v Turkey* (App No 31821/96) (2005) 41 EHRR 27.

[67] supra, note 65 paras 138-139.

[68] ibid, paras 133-137.

[69] ibid.

[70] *Jaloud v the Netherlands* (App No 47708/08) (2014). The ECtHR found that the victim fell within the personal jurisdiction of the Netherlands, despite the argument that that country's forces acted under the operational control of the UK because he passed through a check point specifically set up for the purpose of asserting authority and control over persons during the military operations.

[71] *Chiragov and Others v Armenia* (App No 13216/05) (2015); *Sargsyan v Azerbaijan*, (App No 40167/06) (2015). The Court adopted an expansive approach when applying the spatial model in these two cases. In its evaluation of the evidence confirming Armenian control over the Nagorno-Karabakh for example, the Court found a high level of Armenian influence in the region (including military, political and financial) and consequently effective control over it.

[72] Marko Milanovic, 'Jurisdiction and Responsibility: Trends in the Jurisprudence of the Strasbourg Court', in Anne van Aaken and Iulia Motoc (eds), *The ECHR and General International Law* (Oxford University Press, forthcoming).

[73] UNHRC General Comment No. 35, supra note 58; UNHRC 'Concluding Observations on the Fourth Periodic Report of the United States of America', supra note 61.

well be persuaded to do so, especially in the light of recent explicit acknowledgements from both the HRC and the UN General Assembly that extraterritorial surveillance raises human rights concerns.[75] In particular, the UN High Commissioner for Human Rights report on *The Right to Privacy in the Digital Age*[76] noted the circumstances when human rights obligations may be engaged in the context of extraterritorial surveillance. This will arise in relation to any person, irrespective of their nationality, or physical location whenever a state exercises effective control over the technical, or physical means through which privacy rights are interfered with, for example by direct tapping or penetration of the infrastructure, irrespective of whether or not the state exercise power or effective control over the individual rights bearer as such.[77] The US Upstream[78] and the UK Tempora programmes are designed to do exactly that and therefore in all probability engage these countries' obligations under ICCPR (UK and US) and ECHR (UK). The same applies to the US PRISM, as it allows to directly access the servers of third parties that physically control the data, including Google, Microsoft and Yahoo. In addition Special Rapporteur Ben Emmerson QC was clear on this point observing that '[state's jurisdiction] is not only engaged where State agents place data interceptors on fibre-optic cables travelling through their jurisdictions, but also where a State exercises regulatory authority over the telecommunications or Internet Service Providers that physically control the data'.[79]

---

[74] There are three currently pending cyber surveillance cases before the ECtHR, all alleging breach of Article 8 ECHR by GCHQ following Edward Snowden revelations-
Bureau of Investigative Journalism and Alice Ross v UK (App No 62322/14);
Big Brother Watch and Others v UK (App No 58179/13);
10 Human Rights Organizations v UK (App No Index No IOR 60/1415/2015).

[75] UNHRC, 'Concluding Observations on the Forth Periodic Report of the United States of America', supra note 61.

[76] UNGA, 'Report of the Office of the United Nations High Commissioner for Human Rights the Right to Privacy in the Digital Age' UN Doc A/HRC/27/37 30 (2014).

[77] ibid, para 34:

> […] 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, for example through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State would have obligations under the Covenant.

[78] The Washington Post, 'NSA Slide Shows Surveillance of Undersea Cables' (2013) <https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html>. Upstream collection programmes allow access to very high volumes of data both inside and outside the US and has been described as the 'collection of communications on fibre cables and infrastructure as data flows past' and is conducted under the following four major surveillance programmes- Fairview, Blarney, Stormbrew and Oakstar.

[79] UNGA, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms whilst Countering Terrorism Ben Emmerson QC' (23 September 2014) UN Doc A/69/397 para 41.

3. Cyber Surveillance as an Interference with the Right to Privacy of Communications

Article 17 ICCPR prohibits 'arbitrary or unlawful interference with privacy, home or correspondence'[80] and obliges all state parties to create legal frameworks for the effective protection of privacy including adequate complaint systems, as well as remedies for the violation of this right. The HRC made it clear that 'confidentiality of correspondence should be guaranteed *de jure* and *de facto'*. [81] Correspondence 'should be delivered to the addressee without interception and without being opened or otherwise read'.[82] The Committee's interpretation of the scope of the term 'correspondence' clearly covers NSA/GCHQ cyber surveillance of digital communications, as the term includes all electronic communications, such as email,[83] instant messages, together with telephonic and telegraphic communications.[84] Electronic surveillance, wire-tapping and the recording of conversations is prohibited.[85] In addition, the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals, must be subject to appropriate state regulation and safeguards.[86] The HRC interpreted the phrase 'interference' broadly, to include any measure that either directly, or indirectly infringes on an individual's privacy interests.[87] For these reasons, it is very likely that both NSA and GCHQ surveillance practices interfere with privacy because the mere collection and storage of data, including that which is publically accessible, constitutes an interference falling within the ambit of Article 17 ICCPR.
Similarly, Article 8 ECHR protects everyone's private life, home and correspondence from interference by a public authority, except on specific grounds provided in subparagraph 2. [88] The extent of interference with the right to privacy in the context of states' secret surveillance operations has been subject to an extensive analysis of the ECtHR on a number of occasions. A series of early cases dealing with the interception of telephone conversations applying various surveillance techniques by law enforcement agencies helped to develop a number of principles. Such cases as *Klass and Others v Germany,*[89] *Malone v United Kingdom*,[90] *Halford v United Kingdom*[91] and *Liberty and Others v United Kingdom*[92]

---

[80] ICCPR art 17, supra note 8.
[81] UNHRC, 'General Comment No. 16: Article 17 (Right to Privacy). The Right to Respect of Privacy, Family, Home, and Correspondence and Protection of Honour and Reputation' (8 April 1988) UN Doc HRI/GEN/1/Rev para 8.
[82] ibid.
[83] UNHRC, 'Concluding Observations on Sweden' (2009) UN Doc CCPR/C/SWE/CO/6.
[84] UNHRC General Comment No. 16, supra note 81 para 8.
[85] ibid.
[86] ibid, para 10.
[87] UNHRC *Tooten v Australia* (Communication No 488/1992) UN Doc CCPR/C/50/D/488/1992 (1994). The HRC concluded that the continued existence of the challenged provisions of the Tasmanian Criminal Code continuously and directly 'interfered' with the right to privacy, para 8.2.
[88] ECHR art 8, supra note 9.
[89] *Klass and Others v Germany* (App No 5029/71) (1978) 2 EHRR 214.
[90] *Malone v United Kingdom* (App No 8691/79) (1985) 7 EHRR 14.
[91] *Halford v United Kingdom* (App No 20605/92) (1997) 24 EHRR 523.

established, *inter alia*, that wire tapping of telephone conversations, as well as the use of covert surveillance technologies invariably engages Article 8, since the notion of 'private life' and 'correspondence' extends to the interception of telephone communications and 'metering' practices.[93] In *Liberty* the ECtHR explicitly stated that e-mail communications are also included in the ambit of 'private life' and 'correspondence'.[94] The Court also ruled on the collection and storage of personal data by public authorities.[95] Additionally, in *Weber and Saravia v Germany*[96] and *Kennedy v UK*[97] the ECtHR held that the legislation, which by its mere existence entails a threat of surveillance for all those, to whom it might be applied, impacted on freedom of communication between the users of the telecommunications services and thereby amounted in itself to an interference with the exercise of the rights under Article 8 ECHR. Most recently, the ECtHR engaged with domestic mass surveillance regimes in *Roman Zakharov v Russia*[98] and *Szabo and Vissy v Hungary.*[99] In *Zakharov*, the Grand Chamber of the ECtHR held that the Russian system for permitting surveillance across mobile networks in the interests of crime prevention, which required the network operators to install equipment allowing the interception of all telephone communications without prior judicial authorisation, violated Article 8. *Szabo* concerned surveillance powers of the Hungarian intelligence agency contained in the Police Act 1994 (s 7/E(3)), including interception of electronic or computerised communications without the consent of the person concerned on anti-terrorist grounds. These powers were subject to ministerial, rather than judicial authorisation. They were not linked to a particular crime and required a warrant to relate only to premises, persons concerned, or 'a range of persons', being therefore potentially executable against any person. Given the fact that the scope of the measures could include virtually everyone in Hungary, that the ordering was entirely in the guise of the executive without an assessment of whether interception was strictly necessary, that new technologies enabled the Hungarian government to intercept vast amounts of data concerning even persons outside the original range of operations, together with an absence of any effective remedial measures, the Court concluded that there had been a violation of Article 8.[100] Theses latest judgements reinforce the ECtHR antagonism towards mass surveillance and signal its willingness to take a hard line in the currently pending cases against the UK government, including the *Big Brother Watch*.[101]

---

[92] *Liberty and Others v United Kingdom* (App No 58243/00) (2009) 48 EHRR 1.

[93] supra, note 90. 'Metering' in *Malone* involved the use of a meter to register the number dialled, the time and duration of each telephone call.

[94] supra note 92.

[95] See for example: *Leander v Sweden* (App No 9248/81) (1987) 9 EHRR 433; *S and M Marper v UK* (App No 30562/04) (2008) ECHR 1581; *Shimovolos v Russia* (App No 30194/09) (2011).

[96] *Weber and Saravia v Germany* (App No 54934/00) (2006).

[97] *Kennedy v the United Kingdom* (App No 26839/05) (2010).

[98] *Roman Zakharov v Russia* (App No 47143/06) (2015) ECHR 1065.

[99] *Szabo and Vissy v Hungary* (App No 37138/14) (2016).

[100] European Court of Human Rights Registry, 'Hungarian Legislation on Secret Anti-Terrorist Surveillance Does not Have Sufficient Safeguards Against Abuse' (2016) <http://statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY-prel.pdf.>.

[101] supra, note 74.

4. Can Mass Cyber Surveillance Be Justified?

In one word-no. Any justification put forward by the US and UK authorities must satisfy the requirements of Article 17 ICCPR and Article 8(2) ECHR. Unlike Article 8(2), Article 17 does not provide specific grounds limiting the right to privacy. However, as other non-absolute rights, Article 17 may be limited by proportionate measures designed to achieve a valid aim.[102] Based on the practice of the HRC,[103] as well as the wording of Article 8(2) and its interpretation by the ECtHR, the test for permissible limitations boils down to three main criteria, namely (a) 'in accordance with the law'; (b) legitimate aim and (c) necessity and proportionality.

(a) In Accordance with the Law

Article 17 ICCPR prohibits 'unlawful' interference, meaning that 'no interference can take place except in cases envisaged by the law',[104] which itself must comply with the objectives of the Covenant[105] and 'be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion.'[106] The provision of 'in accordance with the law' in Article 8(2) ECHR similarly requires that surveillance measures must have 'some basis in domestic law', be accessible to the person concerned, be foreseeable as to its effects,[107] as well as being relatively detailed.[108]
The use of surveillance programmes, including Tempora do not meet these standards. First, there are very few states that have so far enacted primary legislation explicitly authorising such programmes.[109] For example, there is no UK statute to date specifically authorising

---

[102] Sara Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights. Cases, Materials and Commentary* (Oxford University Press 2014) 538.
[103] UNHRC General Comment No. 16, supra note 81 paras 3,4,8; UNHRC, 'General Comment 27. Freedom of Movement (Article 12)' (1999) UN Doc CCPR/C/21/Rev.1/Add.9 paras 14-15; *Tooten v Australia* supra note 87 para 8.3.
[104] UNHRC General Comment No. 16, supra note 81 para 10.
[105] ibid para 3.
[106] UNHRC, 'General Comment No. 34. Article 19: Freedoms of Opinion and Expression' (2011) UN Doc CCPR/C/GC/34 para 25.
[107] *Zakharov v Russia*, supra note 98.
[108] ibid, para 231. *Zakharov* reiterated the Court's requirements set out in its earlier jurisprudence, in such cases as *Huvig v France* (App No 11105/84) (1990) 12 EHRR528; *Klass v Germany* supra note 89; *Amman v Switzerland* (App No 27798/95) (2000) 30 EHRR 843; *Weber v Germany* supra note 96. The domestic statute must specify: (a) the categories of people liable to interception; (b) the nature of the offences which may give rise to an interception order; (c) limits of its duration (d) the procedures to be followed for examining, using and storing the data obtained; (e) the precautions to be taken when communicating the data to other parties, and (f) circumstances in which data obtained may, or must be erased or destroyed.
[109] Report of the Special Rapporteur Ben Emmerson, QC supra, note 79 para 37.

interception of communications involving the tapping of the undersea fibre-optic cables. RIPA, aimed at the interception of domestic and foreign telephone communications, has been simply adapted to the new reality of intercepting all internet traffic. So long as one end of a communication is outside the UK, RIPA warrants authorising 'external' communications. However, the distinction between 'external' and 'internal' communications in the context of digital communications is purely theoretical and makes no real difference in practice as to what information may be collected. As a result, the exact legal basis for these powers are unknown and not readily accessible, whilst their is vague and unforeseeable. The UK government has acknowledged in the 2014 litigation against it in the Investigatory Powers Tribunal that it 'considers that an "external communication" occurs every time a UK based person accesses a website located overseas, posts on a social media site overseas such as Facebook, uses overseas cloud storage or uses on overseas email provider such as Hotmail or Gmail. Searches on Google are counted as external communications.'[110] Furthermore, the UK powers to bulk intercept external communications seem to have been used to monitor also domestic data. Indeed, at one point GCHQ was reportedly obtaining 85% of all UK domestic traffic, including internet, via the international cables (using Tempora).[111] Secondly, thus far the UK government has not satisfactorily justified the difference in treatment when collecting 'internal' and 'external' communications to establish that the latter practice is not discriminatory in line with requirement of proportionality set out by the HRC in its General Comment No. 18[112] and the ECtHR in *Burden v UK*.[113] Therefore, the same principles regarding 'in accordance with the law' recently reiterated in *Zakharov* and *Szabo* in relation to domestic powers of surveillance must also apply to foreign, or external communications. On these bases alone, the continued practice of intercepting all external communications under RIPA fails this test, as there is no regard for the procedural safeguards against arbitrary interference by public authorities. For example, as bulk interception by its very nature does not specify the target, this breaches the obligation to identify the categories of people liable to interception and provides no limits on its duration. In *Szabo* the Courts specifically noted that under s 7/E it was possible for virtually any person in Hungary to be subjected to secret surveillance, as the legislation did not describe the categories of persons who in practice may be targeted. The only requirement was for the authorities to name the individuals, or the 'range of persons' to be intercepted to the responsible government minister, without demonstrating their actual, or presumed relation to any terrorist threat. Thirdly, The UK government has already been challenged on the legality of the interception of external communications based on Interception of Communications Act 1985 (ICA) in *Liberty v UK*.[114] The ICA did not indicate with sufficient clarity the scope, or manner of the

---

[110] *Liberty v GCHQ* [2014] UKIPT rib 13_77-H.
<https://www.liberty-human-rights.org.uk/sites/default/files/The%20Intelligence%20Services%20open%20response%20to%20Liberty's%20and%20Privacy%20International's%20claims%2015th%20November%202013.pdf>.

[111] The Guardian, 'MI5 Feared GCHQ Went "Too Far" Over Phone and Internet Monitoring', (2013) <https://www.theguardian.com/uk/2013/jun/23/mi5-feared-gchq-went-too-far>.

[112] supra note 40.

[113] supra note 42.

exercise of surveillance and was therefore not 'in accordance with the law'. Its successor, RIPA, is strikingly similar and will almost certainly fall foul of Article 8 on the same grounds.

Likewise, s 702 FAA, designed ostensibly for an interception of foreign targets, does not satisfy the legality requirement, as it establishes a regime that allows the US government to conduct mass surveillance, including the communications of American citizens, without a warrant, or particularized suspicion.[115]

Clearly, the scope of what has been collected under Article 8(4) RIPA and s 702 FAA is unclear, as both statutes confer very broad discretion on the state agencies, allowing them not only to conduct untargeted surveillance abroad, but also to circumvent the requirements for legitimate use of surveillance powers at home. In that sense both provisions lack the necessary qualities of law.

(b) Legitimate Aim

A state must justify any interference on the basis of the specified legitimate aim. Article 17 ICCPR does not enumerate an exhaustive list of public policy objectives that may form the basis of such a justification. Nevertheless, the prevention, suppression and investigation of acts of terrorism have been held to amount to a legitimate aim for the purposes of Article 17.[116]

Unlike Article 17 ICCPR, Article 8(2) ECHR does provide a list of legitimate aims, among them the interest of national security and economic well being of the country.[117] As a general principle, the existence of legislation granting powers of secret surveillance over communications including email is necessary in the interest of national security.[118] In addition, it has been held that the enhanced capacity of states to monitor all internet traffic has been recognized as a valid 'basis of an arguable justification for mass surveillance of the Internet' in the interest of prevention and suppression of global acts of terrorism.[119] However, states do not enjoy an unlimited discretion to subject persons within their jurisdictions to secret surveillance and may not, in the name of the struggle against espionage and terrorism adopt whatever measures they deem appropriate.[120] Indeed, such measures are only tolerable in so far as the means provided for by the legislation to achieve these aims remain within the bounds of what is necessary in a democratic society.[121] Lately,

---

[114] *Liberty v UK*, supra note 92. The case concerned the interception of communications authorised by the Ministry of Defence of Liberty and other human rights groups between 1990-97.

[115] Electronic Frontier Foundation, 'Section 702 of the Foreign Intelligence Surveillance Act (FISA): Its Illegal and Unconstitutional Use' <https://www.eff.org/files/filenode/702_one_pager_final_adv.pdf.>. The FISC approved PRISM orders directed at specific companies have been sued to access Americans' communications, so long as the order targets at least 51% of foreign people.

[116] Report of the Special Rapporteur Ben Emmerson QC, supra note 78 para 33.

[117] Art 8, supra note 3.

[118] *Klass v Germany*, supra note 89 para 48; *Leander v Sweden*, supra note 95 para 59.

[119] Special Rapporteur Ben Emmerson QC, supra note 79 para 34.

[120] *Klass v Germany*, supra note 89, para 49.

[121] ibid, paras 46 and 49.

in *Zakharov* the ECtHR's Grand Chamber rejected surveillance authorised on 'national, military, economic or ecological security grounds' for being insufficient, requiring that any authorisation must be based on a 'reasonable suspicion against a person concerned'.[122] This means that when authorising surveillance measure, an authorising body must be capable of verifying whether there are factual indications for suspecting that person of planning, committing, or having committed criminal act or acts endangering national security.[123] The 'reasonable suspicion' approach was not only endorsed, but also further elaborated on by the ECtHR in *Szabo* earlier this year. The phrase 'necessary in a democratic society' now requires that any secret surveillance must be strictly necessary in two senses: (a) as a general consideration for the safeguarding of democratic institutions; and (b) as a particular consideration for the obtaining of vital intelligence in an individual operation.[124]

The official justifications by the US and UK governments regarding untargeted foreign surveillance are rare and mainly based on national security grounds, in particular fighting and preventing terrorism and crime.[125] As such these grounds are too broad and unspecific and therefore do not meet the criteria of 'reasonable suspicion'. Instead, they bear all the hallmarks of 'fishing expeditions' that the ECHtR is particularly adverse to.[126]

(c) Necessity and Proportionality of Mass Surveillance

States must demonstrate that any interference with the right to privacy under Article 17 ICCPR and Article 8(2) ECHR is a necessary means to achieving a legitimate aim. Establishing that the interference is necessary requires from a state to show not only that the interference with a person's right meets a pressing social need, but that it is also proportionate to the legitimate aim pursued.[127] This means that the interference cannot be greater than is necessary to address that pressing social need.[128] Additionally, the measure

---

[122] *Zakharov v Russia*, supra note 98 para 260.
[123] ibid.
[124] *Szabo v Hungary*, supra note 99 para 98.
[125] US House of Representatives Permanent Select Committee on Intelligence, 'Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programs Protect Americans and Why Disclosure Aids Our Adversaries' (2013) < https://www.hsdl.org/?view&did=739351>;The Huffington Post, 'Barak Obama Justifies PRISM NSA Surveillance Programme Saying it Has Saved Lives' (2013) <http://www.huffingtonpost.co.uk/2013/06/19/prism-obama-germany-merkel_n_3464613.html>.
[126] Vinci Construction and GTM Genic Civil et Services v France (App No 63629/10 & 60567/10) (2015). 'Fishing expeditions' are searches, or investigations undertaken in the hope of discovering information, whereby data in mined to identify possible terrorist/criminal activity rather than the actual activity. In *Vinci* the ECtHR held that unannounced inspections, searches and seizures of computer files for the purposes of an official investigation by the French competition authority violated Article 6(1)-right to fair trial, as well as Article 8.
[127] Bernadette Rainey et al., *The European Convention on Human Rights* (Oxford University Press 2014) 325.
[128] ibid.

in question must be the least intrusive instrument amongst those, which might achieve their protective function.[129]

In the case of intrusion into internet privacy rights, proportionality involves balancing the extent of the intrusion against the specific benefits accruing to investigations undertaken by public authority in the public interest.[130] The principle of proportionality seems not to be satisfied in cases of the use of mass surveillance programmes by both the US and the UK authorities under Article 17 ICCPR. One reason is that the official success rate in fighting/preventing terrorism appears insignificant in relation to the scale of surveillance operations. The figures declared by the Obama Administration justifying their use of PRISM set the number of prevented terrorist threats at at least fifty,[131] but these claims have been subsequently discredited. In *Klayman v Obama*[132] the court found that the US government was unable to 'cite a single case in which analysis of the NSA's bulk metadata collection actually stopped an imminent terrorist attack'.[133] In addition, US President's Review Group on Intelligence and Communications Technologies evidenced that mass surveillance impedes law enforcement efforts and recommended that significant steps should be taken to protect privacy of non-US persons.[134] In particular, it refuted the Administration's claims regarding the number of lives saved as a result of metadata collection, advising that the bulk surveillance programmes should be shut down.[135] Similarly, according to the PACE report, mass surveillance does not appear to have contributed to the prevention of terrorist attacks, contrary to earlier assertions made by senior intelligence officials.[136]

Similar conclusion can be reached in the light of the ECtHR jurisprudence regarding the assessment of proportionality. In *Leander v Sweden*[137] the ECtHR accepted that states should enjoy wide discretion, both in assessing the existence of a pressing social need and in choosing the means of achieving the legitimate aim of protecting national security. However, in *Klass*[138] and later in *Zakharov*, [139] the ECtHR emphasised that states do not enjoy

---

[129] UNHRC General Comment No. 34, supra note 106 para 34.

[130] supra note 79, para 51.

[131] Joan McCarter, 'President Obama: 'Lives Have Been Saved' (2013) <http://www.dailykos.com/story/2013/6/19/1217312/-President-Obama-Lives-have-been-saved-by-NSA-surveillance>.

[132] *Klayman v Obama* 957 F Supp 2d. 1 (2013).

[133] Reuters, 'US Court Hands Win to NSA over Metadata Collection' (2015) <http://www.reuters.com/article/us-usa-court-surveillance-idUSKCN0QX1QM20150828>. The decision that the NSA mass collection of phone metadata was unconstitutional was reversed by the US Court of Appeal for the District of Columbia in August 2015.

[134] supra note 18.

[135] ibid, Recommendation 4:

> We recommend that, as a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest.

[136] supra note 6.

[137] supra note 95.

an unlimited discretion to subject persons within their jurisdictions to secret surveillance and may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. Mass data collection programmes therefore appear to offend against the requirement that intelligence agencies must select the measure that is the least intrusive on human rights and thus undermine the very essence of the right to privacy.[140]

It could therefore be said that the use of PRISM, Tempora and other such programmes do not seem to have legal basis in domestic law, fail to satisfy the requirement of legitimate aim and are disproportionately intrusive. For these reasons they are in all probability unlawful under Article 17 ICCPR and Article 8 ECHR.

The Future of Mass Surveillance

The future of the internet as a medium for free and open exchange of information globally has been seriously undermined, as evidenced by the political fallout. To begin with, revelations that the NSA spied on even its closest allies have affected state-to-state relationships, with the Brazilian, German and Indian authorities expressing their outrage in the immediate aftermath.[141] The trend for more 'technological sovereignty' and 'data nationalization' has also intensified, with both Brazil and the European Union recently announcing plans to lay a $185 million fibre-optic cables between them to thwart US surveillance.[142]

A number of international and regional institutions have also acted swiftly in condemning mass surveillance. The UN General Assembly (UN GA), the Human Rights Council and the UN Office of the High Commissioner for Human Rights (OHCHR) have gone to a considerable effort to address these issues. The UN GA adopted two Resolutions on the right to privacy- 68/167[143] and 69/166,[144] both affirming that people's rights protected offline should also be safeguarded on line. The OHCHR presented a report in June 2014, which

---

[138] supra note 89 para 48. The ECtHR recognized that 'democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction'.
[139] *Zakharov*, supra note 98 para 49.
[140] supra note 79, para 52.
[141] supra note 6, paras 104-105.Brazilin President Rousseff has strongly condemned NSA surveillance at an address before the UN General Assembly in September 2013, whilst German *Der Spiegel* accused the NSA of 'turning the internet into a weapons system' following the revelations of spying on the Chancellor Merkel and other high-profile Germans. On 2 July 2014 India summoned a senior US diplomat over reports that the US had authorised the NSA to spy on the ruling party, the BJP, in 2010 when it was in the opposition.
[142] ibid, para 108.
[143] UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167.
[144] UNGA Res 69/166 (18 December 2014) UN Doc A/RES/69/166.

spelled out the violations of privacy in the context of Article 17 ICCPR, stating that governmental surveillance 'is emerging as a dangerous habit rather than an exceptional measure'.[145] In 2015 the Human Rights Council adopted Resolution 28/16 appointing a Special Rapporteur on the rights to privacy, Professor Joseph Cannataci, with the mandate to report on alleged violations of this right including in connection with the challenges arising from new technologies.[146]

(a) Regulation of the Activities of Intelligence Agencies

The first concrete proposal to date from an international organization to address the working methods of intelligence services in the sphere of digital communications came from the Council of Europe (CoE) in the form of the Intelligence Codex. Four simple rules were suggested for governing co-operation among the intelligence agencies. First, any form of mutual political, economic espionage must be prohibited without exception.[147] Secondly, any intelligence activity on the territory of another member state would only be carried out with that state's approval and within a statutory framework, that is for a specific reason of preventing crime/terrorism.[148] Thirdly, the tracking, analysing and storing of mass data is strictly prohibited if that data is from non-suspected individual from a friendly state. Only information pertaining to legitimately targeted individuals may be collected on an exceptional basis for specific individual purposes, whilst any data that is stored, but not needed must be immediately destroyed.[149] Finally, the intelligence agencies would be banned from forcing telecommunication and internet companies to grant them unfettered access to their massive databases of personal data without a court order.[150]

There can be no doubt that a binding treaty, such as the proposed Codex is necessary. The Council of Europe has provided a number of reasons as to why such an instrument is desirable. Among them, rebuilding trust among transatlantic partners, member states of the CoE, as well as between citizens and their governments was considered to be of outmost importance. [151] Moreover, 'the political problems caused by "spying on friends" and the possible collusion between intelligence services for the circumvention of national restrictions show the need for states to come up with a generally accepted "codex" for intelligence agencies that would put and end to unfettered mass surveillance and confine surveillance practices to what is strictly needed for legitimate security purposes'.[152]

That being the case, the question is how feasibly is it that such a treaty be adopted? So far states showed no real appetite to regulate peacetime espionage (be it in its traditional or cyber form) through an internationally binding treaty.[153] As a consequence,

---

[145] UNCHR, Twenty-seventh Session 'Report of the UN High Commissioner for Human Rights on the Right to Privacy in the Digital Age' (30 June 2014) UN Doc A/HRC/27/37.
[146] UNGA Res 28/16 (24 March 2015) UN Doc A/HRC/28L.27.
[147] supra note 45, 50.
[148] ibid.
[149] ibid.
[150] ibid.
[151] ibid, para 13, 8.
[152] ibid, para 115, 50.

international law has been rather ambivalent regarding regulation of electronic surveillance, which falls within the broader concept of peacetime espionage.[154] However, there has been a marked shift in focus in relation to who is the subject of surveillance. Historically, signals intelligence efforts were concentrated on gathering data about decision making in foreign governments.[155] Colleting information on private individuals was not wide-spread and also costly. Consequently, public pressure to curtail espionage was minimal as it was not seen to effect average citizens abroad.[156] This has dramatically changed and may encourage at least some states to consider putting on express legislative footing how, when and where foreign governments may intercept their citizens' communications. However, a global international legal framework for surveillance coming to fruition any time soon is very much in doubt. This is compounded by a lack of blueprint that can serve as a yardstick for such a treaty. This does not necessarily mean that a multilateral treaty could not be achieved on a smaller scale, originating in the Council of Europe. The CoE has a successful track record regarding the negotiation of international treaties, as demonstrated by the Convention on Cybercrime 2001 (the Budapest Convention)[157] and Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108),[158] both dealing with activities conducted in the cyber environment. They begun life as regional, European instruments, but in time became international, albeit not universal, since they allow for accession by non-European countries. Thus, the Budapest Convention has been ratified by 49 parties, among them four non-Council of Europe states who signed it (the US, Canada, Japan and South Africa) and five, including the US which also ratified it.[159] Similarly, the 'globalization' of Convention 108 beyond its European origins has been underway since the start of this decade, when Uruguay acceded to it in 2013.[160] The expansion of Convention 108 is set to continue with Mauritius depositing its instruments of accession this year and other four non-European countries (Cape Verde, Morocco, Senegal and Tunisia) at various stages of the process.[161] The Intelligence Codex too could not only become a regional treaty, but also provide an opportunity to other non-European states to become a party to it and thus have wider than Europe reach.

---

[153] For an overview see Deeks, supra note 5.

[154] The US FISA defines electronic surveillance to include 'the acquisition by an electronic, mechanical, or other surveillance devices of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs within the Unite States'. 50 USC §1801(f)(2).

[155] supra note 5, p 23.

[156] ibid.

[157] Cybercrime Convention [2001] European Treaty Series No 185.

[158] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [1981] European Treaty Series No 108.

[159] Council of Europe Chart of Signatures and Ratifications of Treaty 185 Convention on Cybercrime Status as of 31/07/2016. The other states are Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama and Sri Lanka.

[160] Graham Greenleaf, 'Balancing Globalization's Benefits and Commitments: Accession to Data Protection Convention 108 by Countries Outside Europe' (2016) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2801054>.

[161] ibid.

Thus far, the Intelligence Codex has met with only one, unfavourable response from the 47 CoE member states from the Netherlands. In the absence of more reactions from the member states it is difficult to speculate what the future of the Codex may be. If the proposal fails, an alternative solution could be a voluntary Intelligence Codex.[162] Such soft law option would also have a strong effect, 'because those that do not abide by it could be accused of wrongful actions by their allies, thus eroding their credibility as cooperation partners'.[163] However, as demonstrated by the now annulled *Safe Harbour* agreement, non-legally binding schemes are easier to circumvent than hard law instruments.[164] Undoubtedly, a multilateral binding agreement would be more effective to close loopholes states can currently exploit in order to circumvent legal limits placed on their intelligence programmes, especially in relation to 'collusion for circumvention', which still allows intelligence agencies to push the boundaries of their data collection powers at home by relying on data collected by their allies or third parties.[165]

What could be its advantage though over and above the existing international human rights architecture? There are at least two reasons in support of the Codex, first the need for up to date norms under Article 17 ICCPR and secondly, to supplement the jurisprudence of the ECtHR on Article 8 ECHR. These points will be discussed below.

(i) The Need to Modernise Article 17 ICCPR

Needles to say, each state should prefer a world in which its officials and citizens were less often subject to foreign surveillance.[166] However, to achieve reduced surveillance through an internationally binding treaty states must have clearly defined norms. This at present appears lacking, as the existing international law norms under Article 17 ICCPR, in particular its General Comment No. 16 issued in 1988, have not kept pace with the rapid developments in surveillance and information technologies. As a consequence, the law on privacy is outdated and needs to be modernized.

The past practice of the HRC set a precedent for revising or replacing general comments.[167] The HRC has been motivated by the need to provide greater detail and more authoritative guidance on a content of a particular article, as well as the need to ensure that

---

[162] Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe, 'Explanatory Memorandum by Mr Pieter Omtzigt, Rapporteur' AS/Jur (2015), para 117.

[163] ibid.

[164] Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015]ECJ. The Court of Justice of the European Union held that all data transfers from Facebook's Irish subsidiary to its US headquarters under the EU-US Safe Harbour agreement were unsafe, because the US law did not offer sufficient protection against surveillance by that country's public authorities.

[165] supra note 163.

[166] supra note 5, 21.

[167] supra note 46. In 2011 General Comment No. 10 (written in 1983) was replaced with General Comment No. 34 on Article 19, protecting the right to freedom of expression, whilst in 2013 General Comment No.8 issued in 1982 was replaced with General Comment No. 35 on Article 9, protecting liberty and security of the person.

general comments reflect the changing realities and incorporate developments in the law.[168] General Comment No. 16 is no exception. Although it sets out the core concepts contained in Article 17, it has lagged behind the technological developments in modern communications and surveillance practices. Consequently, new general comment on Article 17 ICCPR must provide explicit articulation of what is the right to privacy of communications in the digital sphere and spell out the content of this right to ensure its effective protection and enforcement. Currently General Comment No. 16 shortcomings relate to the lack of explicit recognition of such matters as banning untargeted, mass surveillance,[169] bulk metadata collection and retention;[170] protecting metadata;[171] intelligence services/law enforcement access to communications data held by third party service providers and internet companies including in a 'cloud'; the relationship between private companies and governments;[172] biometric data gathering (through for example finger printing, facial recognition software) and transborder access to non-publically available data circumventing the requirements of the Mutual Legal Assistance Treaties. In addition, some matters must be settled beyond doubt, such as extraterritorial application of human rights and equal treatment of citizens and foreigners, as well as specifying the circumstances when the right to privacy may be restricted. [173]

(b) The Need to Supplement the ECtHR Jurisprudence under Article 8 ECHR

The PACE report indicated that the Intelligence Codex would adopt the safeguards devised by the European Court of Human Rights for surveillance.[174] However, these safeguards provide only minimum standards[175] that member states must adhere to and need to be reinforced by detailed rules in at least four areas, namely (a) legality- in relation to the so called 'contact chaining'; (b) legitimate aim; (c) judicial authorisation; and (d) complaints mechanism- user notification.

---

[168] ibid.
[169] *Zakharov*, supra note 98; *Szabo*, supra note 99.
[170] Joint Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd and Seitilinger and Others* [2014] ECJ. The CJEU declared that the EU Data Retention Directive, which compelled all internet and telecommunication service provides operating in Europe to obtain and retain subscribers' incoming and outgoing telephone and internet metadata for the period of six months to two years was invalid.
[171] *Copland v the United Kingdom* (App No 62617/00) (2007) ECHR; *Malone* supra note 98; UNHRC Report by the Special Rapporteur Frank La Rue on the Promotion and Protection of the Right to Freedom of Opinion and Expression (17 April 2013) UN Doc A/HRC/23/40.
[172] *Maximilian Schrems v Data Protection Commissioner,* supra note 164.
[173] Special Rapporteur Frank La Rue, supra note 153 para 29; UNHRC Report by Special Rapporteur Martin Scheinin on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism (28 December 2009) UN Doc A/HRC/13/37 para 11. The Special Rapporteurs suggested that the limitations to the right to privacy are subject to the test of permissible limitations set forth by the HRC in its General Comment No. 27 to Article 12 (freedom of movement).
[174] PACE Report, supra note 6 para 97, 80.
[175] ibid 57.

(i) Legality

In such cases *Klass,*[176] *Malone,*[177] *Weber,*[178] *Liberty,*[179] *Rotaru v Romania,*[180] *Zakharov*[181] and *Szabo*,[182] the Strasbourg Court has developed minimum standards, which domestic law must meet in order to be compatible with Article 8 outlined in part 4(a) above,[183] among them the requirement to specify the categories of people liable to have their communication intercepted. In gathering information, state authorities often build a human network around an individual of interest to them by gathering telephone and/or internet metadata related to other persons with whom that individual may be in contact and who are usually one or two stops ('hops') away from him/her. This is known as 'contact chaining'. National legislation would usually set out these powers in terms of 'relevance' for the investigation of terrorism or crime.[184] The Strasbourg Court has not yet addressed this issue in the context of interception of internet metadata,[185] yet in this case the 'relevance' criterion gives potential for expanding the net of surveillance greatly to cover huge numbers of people without any connection whatsoever to crime or terrorism.[186] Contact chaining must therefore be regulated by placing strict limits on the power to query collected bulk metadata.

---

[176] supra note 88.
[177] supra note 89.
[178] supra note 95.
[179] supra note 91.
[180] *Rotaru v Romania* (App No 28341/95) (2000) ECHR 2000-V.
[181] supra note 97.
[182] supra note 98.
[183] supra note 97. These include:

(1) the nature of the offences which may give rise to an interception order;
(2) definition of the categories of people liable to have their telephones tapped and a limit on the duration of telephone tapping;
(3) the procedures to be followed for examining, using and storing of data obtained; the precautions to be taken when communicating the data to other parties; and
(4) the circumstances in which recordings may or must be erased or the tapes destroyed.

[184] Some jurisdictions, for example in the US, the access to stored telephony metadata will be granted on the basis of 'reasonable articulable suspicion' individually approved by the Foreign Intelligence Surveillance Court under s 215 Foreign Intelligence Surveillance Act.
[185] European Commission for Democracy Through Law (the Venice Commission), 'The Democratic Oversight of Signals Intelligence Agencies' (20-21 March 2015), para 98, 81. The Venice Commission explained contact chaining in the following terms:

> The bulk metadata are analysed to identify communications patterns. This usually takes the form of checking whether previously identified suspect telephone numbers (X) are in contact with other numbers (Y) and then whether Y is in contact with other numbers (Z).

[186] ibid, para 10, 57.

(ii) Legitimate Aim

The *Zakharov* and *Szabo* cases illustrate the Court's acknowledgement that the legal threshold of 'national security' is dangerously broad especially in the context of mobile/electronic communications, which contrasts with its earlier more permissive approach in *Weber* and *Kennedy*. The ECtHR now favours a stringent test based on reasonable suspicion and this criterion should be adopted in the Codex, as a legal requirement for all surveillance powers. As for allowing the collection of signals intelligence for 'economic well being of the country', it has been feared that this may give rise to the suspicion of economic espionage.[187] The problem is that there seems to be no limits set out by the ECtHR jurisprudence regarding when data may be collected pursuant to this ground. One view was that to avoid nations acting for nefarious purposes cloaked in the 'economic well being', this criterion must be accompanied by clear prohibition of economic espionage, buttressed by effective oversight and prohibitions on letting government departments, or administrative agencies concerned with promoting trade, task the signals intelligence agencies.[188]

(iii) Judicial Authorisation

In order to comply with the ECHR a secret surveillance programme must be subject to independent supervision, which may be either judicial or non-judicial.[189] In its past cases, the ECtHR held that judicial authorisation is 'in principle desirable and 'offer[s] the best guarantee of independence, impartiality and a proper procedures',[190] but stopped short of requiring this in all circumstances. In *Klass* the ECtHR found that oversight by a non-judicial body was allowed, where that body is sufficiently 'independent of the authorities carrying out the surveillance'.[191] Yet, the issue of impartiality in cases where authorisation has been in the guise of a non-judicial bodies, such as an official of the Post Office, gave the Court reasons for concern.[192] An opportunity to require that all states must provide that only judicial authorisation would suffice arose lately in *Zakharov*, but the Court held that 'control by an independent body, normally a judge with special expertise, *should* be the rule and substitute solution, the exception warranting close scrutiny'.[193] *Szabo* was yet another confirmation that judicial control of secret surveillance is preferable, but not obligatory.[194] In

---

[187] ibid.

[188] ibid para 73, 73.

[189] *Weber* supra note 95; *Klass* supra note 88; *Zakharov* supra note 97; *Szabo* supra note 98.

[190] *Klass*, supra note 88 para 87.

[191] ibid para 56.

[192] Kopp v Switzerland (App No 23224/94) (1999) 27 EHRR 91, para 74:

> It is, to say the least, astonishing that [the] task [of authorising interceptions] should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge…

[193] *Zakharov,* supra note 97 para 77.

[194] *Szabo*, supra note 98 para 75. The ECtHR opined that judicial authorisation offers the best guarantees of independence, impartiality and a proper procedure, since the supervision of a

the sphere of mass surveillance, the key defect therefore of the current authorisation regime is the Court's repeated reticence to make the requirement of judicial authorisation mandatory across jurisdictions.

(iv) Complaints Mechanism

Under Article 13 ECHR individuals have a right to an effective remedy in their national courts in cases where a public authority has infringed their Convention rights.[195] Part of this entitlement is the right of citizens to be informed of their data being collected and/or that they have been subject of surveillance, known as user notification.[196] However, the issue of whether and when an individual may expect to be informed is far from settled. In *Klass*, the ECtHR found that states are not required to disclose that they have ordered or conducted surveillance in a particular case, nor must they notify a person after the surveillance has ceased.[197] The ECtHR considered that is was not feasible in practice to require post interception notification in all cases.[198] In the subsequent cases the ECtHR showed a clear tendency towards the establishment of this as a right. [199] For example, in *Ekimdzhiev* v Bulgaria[200] the ECtHR held that the missing notification of the individual after surveillance violated both Article 8 and Article 13 ECHR, but fell short of finding that notification was a necessary requirement of domestic surveillance laws in general, stating that authorities *should* issue a notification to an individual who had been secretly monitored.[201]

Conclusion

The extent of mass foreign surveillance exposed by Edward Snowden in 2013 reinforced the need to safeguard human rights in the online environment. Whilst the political dust on mass surveillance is slowly settling down, what has become apparent is a series of shortfalls in the international legal framework on privacy of communications when applied to the digital sphere. Although in principle privacy laws apply therein, Article 17 ICCPR and Article 8 ECHR are either outdated and/or require additional standards, matching the demands of modern gathering of signals intelligence. Equally, the move towards greater surveillance powers in

---

member of the executive (the Minister of Justice) did not provide the necessary guarantees against abuse.

[195] ECHR, supra note 9 art 13.

[196] Necessary and Proportionate, 'Global Legal Analysis. Background and Supporting International Legal Analysis for the International Principles on the Application of Human Rights to Communications Surveillance '(2014) <https://necessaryandproportionate.org/global-legal-analysis>, 24.

[197] *Klass*, para 88.

[198] ibid para 58.

[199] *Weber*, supra note 95; *Association for European Integration and Human Rights and Ekimdzhiev and Bulgaria* (App No 62540/00) (2007); *Kennedy,* supra note 96; *Uzun v Germany (*App No 36623/05) (2010); *Zakharov*, supra note 97.

[200] ibid.

[201] supra note 181, 24.

some European countries and the US as a result of an increased number of terrorist attacks suggests that the calls from the UN organizations and human rights bodies have been ignored. Yet, mass untargeted surveillance does not work in preventing serious crime and terrorism and is unlawful under international human rights law. This problem remains inadequately dealt with, despite the calls from the UN General Assembly and the Human Rights Council to put a stop to these practices. This therefore calls for a more robust solution, such as the one proposed by the Council of Europe in the form of a multilateral binding treaty that aims to ban all forms of economic, political and diplomatic espionage. This paper not only came in support of such a hard law solution, but also proposed that foreign untargeted cyber surveillance conducted on unspecified grounds and without an independent judicial authorisation, must be prohibited.