

2017 9th International Conference on Cyber Conflict

Defending the Core

H.Röigas, R.Jakschis, L.Lindström, T.Minárik (Eds.)

2017 © NATO CCD COE Publications, Tallinn

Permission to make digital or hard copies of this publication for internal use within NATO and for personal or educational use when for non-profit or non-commercial purposes is granted providing that copies bear this notice and a full citation on the first page. Any other reproduction or transmission requires prior written permission by NATO CCD COE.

# The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance

**Eliza Watt**

Westminster Law School  
University of Westminster  
London, UK  
[elizawatt@googlemail.com](mailto:elizawatt@googlemail.com)

**Abstract:** Whilst the political dust on mass surveillance is slowly settling down, what has become apparent is the uncertainty regarding the interpretation and application of the right to privacy norms under Article 17 of the International Covenant on Civil and Political Rights 1966 in the context of cyberspace. Despite the world-wide condemnation of these practices by, *inter alia*, the United Nations and international human rights organisations, little consensus has been reached on how to bring them in line with international human rights law. This paper proposes that the most pragmatic solution is updating Article 17 by replacing General Comment No.16. There are many issues that require attention. The paper focuses on two fundamental aspects of this process, namely the development of more detailed understanding of what is meant by the right to privacy in the 21st century, and the challenge posed by foreign cyber surveillance to the principle of extraterritorial application of human rights treaties. To that end, the paper identifies that the ‘effective control’ test, developed by international human rights courts and bodies adopted to determine jurisdiction, is unsuitable in the context of state-sponsored cyber surveillance. The paper considers a number of suggestions made by legal scholars, which hinge on the control of communications, rather than the physical control over areas or individuals. Such a ‘virtual control’ approach seems in line with the jurisprudence of the European Court of Human Rights, according to which extraterritorial obligations may arise when states exercise authority and control over an individual’s human rights, despite not having physical control over that individual. The paper argues that the ‘virtual control’ test, understood as a remote control over the individual’s right to privacy of communications, may help to close the normative gap that state intelligence agencies keenly exploit at the moment.

**Keywords:** *cyber surveillance, privacy, extraterritorial obligations, 'effective control' test, 'virtual control' test*

## 1. INTRODUCTION


One of the starkest lessons to be learned from the 2013 Edward Snowden revelations is the need for a global solution regarding state sponsored communications surveillance,<sup>1</sup> conducted in particular by the coalition of the so-called Five Eyes states.<sup>2</sup> Undoubtedly, these activities breach the right to privacy of communications<sup>3</sup> enshrined in Article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR)<sup>4</sup> and Article 8 of the European Convention on Human Rights 1950 (ECHR).<sup>5</sup> However, despite numerous calls from international organisations and human rights courts and bodies condemning mass surveillance, to date there is no consensus on how to bring these activities in line with human rights law.

This paper will address some of these challenges, focusing on legal solutions within the existing international human rights framework, as achieving a legally binding agreement remains elusive. To that end, the first part will outline some recent developments from the United Nations (UN) organisations<sup>6</sup> and human rights bodies;<sup>7</sup> it will conclude that current state practice in the form of transboundary state-sponsored cyber espionage<sup>8</sup> and long-standing disagreements regarding the future of Internet governance<sup>9</sup> make the negotiation from scratch of a new UN privacy treaty for the digital environment unlikely. However, there are other solutions, discussed in part two, such as the long overdue modernisation of the existing privacy norms under Article 17 ICCPR. The paper will focus on two important aspects of this process, namely the updating of the notion of privacy and the extraterritorial application of human rights treaties in the context of cyber surveillance. This part will outline the approach adopted in the international human

<sup>1</sup> For a definition of communications surveillance see UNHRC 'Report by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (2013) UN Doc A/HRC/23/40, para 6.

<sup>2</sup> The Five Eyes comprises the US National Security Agency, the UK General Communications Headquarters, Canada's Communications Security Establishment Canada, the Australian Signals Intelligence Directorate and New Zealand's Government Communications Security Bureau.

<sup>3</sup> UNGA, 'Report of the Office of the United Nations High Commissioner for Human Rights the Right to Privacy in the Digital Age' (2014) UN Doc A/HRC/27/37, para 20; *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIPTrib 15\_11-CH.

<sup>4</sup> International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force March 1976) 999 UNTS 171 (ICCPR), art 17. 

<sup>5</sup> 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.

<sup>6</sup> UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167; UNGA Res 69/166 (18 December 2014) UN Doc A/RES/69/166.

<sup>7</sup> OHCHR Report, supra note 3; UNHRC, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson QC' (2014) UN Doc A/69/397; Report of the Special Rapporteur La Rue, supra note 1.

<sup>8</sup> 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.

<sup>9</sup> *The Guardian*, 'ITU and Google Face-off at Dubai Conference over Future of the Internet' (3 December 2012).

rights law jurisprudence, which in certain circumstances holds a state accountable for human rights violations conducted extraterritorially, based on the ‘effective control’ test. It will be shown that this model of extraterritorial jurisdiction, currently articulated as physical power or control over either an area or a person, is not well suited to the cyber environment and needs therefore to be adapted for the transboundary context of digital mass surveillance. A number of possible solutions have been proposed by legal scholars, and this paper will outline some of their rationales. It will conclude that the exercise of power or authority over an individual’s right to privacy through ‘virtual control’ over their communications may constitute a workable way forward in preventing states from avoiding their human rights responsibilities ‘simply by refraining from bringing those powers within the bounds of the law’.<sup>10</sup>

## HUMAN RIGHTS PROTECTION IN CYBERSPACE

Efforts to construct a global coordination and policy-making framework for the Internet began in the mid-1990s and to date remain unsuccessful.<sup>11</sup> There is no single state, or international body formally in overall charge of ensuring compliance with the law in respect of the way the Internet works.<sup>12</sup> Nor is there an overall treaty applicable to the Internet, although there are national laws and international treaties that are applicable to activities on the Internet.<sup>13</sup> In the context of international security, a broad consensus has been reached by the UN Group of Governmental Experts that, in principle, international law and in particular the Charter of the United Nations apply in cyberspace.<sup>14</sup> The UN Human Rights Council, in adopting Resolutions in 2012, 2014 and 2016,<sup>15</sup> together with the UN General Assembly (GA) adopting Resolutions in 2013 and 2014 on the right to privacy in the digital age, have asserted that international human rights law applies as much offline as online.<sup>16</sup> To that end, Resolution 69/166 called upon member states to review their practices and legislation on the interception and collection of personal data, including mass surveillance, to ensure the full and effective implementation of their obligations under international human rights law. Resolution 28/16 in 2015 also urged states to provide ‘an effective remedy’ and encouraged the Human Rights Council to identify ‘principles, standards and best practice’ for protection of privacy.<sup>17</sup>

The protection of human rights online has been a subject of international Internet governance<sup>18</sup> discourse for some time, including during the World Summit for the Information Society in 2003 and 2005. Not until the Snowden revelations, however, did the need for increased privacy protection gain importance and, subsequently, calls for the setting of international norms in

<sup>10</sup> Supra note 3, para 33.

<sup>11</sup> Milton Mueller, et al. ‘The Internet and Global Governance: Principles and Norms of a New Regime’ (2007) 13 Global Governance.

<sup>12</sup> Council of Europe Commissioner for Human Rights, ‘The Rule of Law on the Internet and in the Wider Digital World’ (2014), 36.

<sup>13</sup> Council of Europe, Convention on Cybercrime (23 November 2001) ETS No 185; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1 October 1985) ETS 108.

<sup>14</sup> UNGA, ‘Report by Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security’ (24 June 2013) UN Doc A/68/98; UN Doc A/70/174 (22 July 2015).

<sup>15</sup> UNHRC Res A/HRC/RES/20/8 (16 July 2012); UNHRC Res A/HRC/RES/26/13 (14 July 2014); UNHRC Res A/HRC/RES/32/13 (18 July 2016).

<sup>16</sup> UNGA Res 68/167 (n 6).

<sup>17</sup> UNGA Res 28/16 (26 March 2015) UN Doc A/HRC/28/16.

<sup>18</sup> For a definition of Internet governance, see World Summit on Information Society, ‘Tunis Agenda for Information Society’ (2005) WSIS-05/Tunis/Doc/6(Rev. 1), 4.

relation to the interception of communications and data protection intensified. In 2013, the President of the Republic of Brazil, Dilma Rousseff, made a compelling case for the creation of ‘multilateral mechanisms for the worldwide network that are capable of ensuring principles such as freedom of expression, privacy of individuals and respect for human rights’.<sup>19</sup> Germany, leading a coalition of states, also proposed to enshrine digital privacy in an international human rights treaty by means of a new additional protocol to Article 17 ICCPR for the ‘digital sphere’.<sup>20</sup> The idea, put forward at the 35th International Conference of Data Protection and Privacy Commissioners, was overwhelmingly supported by most of the privacy authorities, except for the United States (US).<sup>21</sup> Nevertheless, the opening of the negotiations on the additional protocol to Article 17 ICCPR conducted by the Special Rapporteur on Privacy, Professor Cannataci has begun.<sup>22</sup> The additional protocol is not envisaged, however, as ‘one new global all-encompassing international convention covering all of privacy or Internet governance’.<sup>23</sup> The Special Rapporteur adopted a realistic approach, expecting that protection of privacy could be increased by incremental growth of international law through the clarification and eventually the extension of existing legal instruments. This seems to be a pragmatic solution, bearing in mind the number of unsuccessful attempts to reach an international agreement regarding the setting out of norms regulating state behaviour in cyberspace, in particular those of the Shanghai Cooperation Organisation in 2011 and 2015 introducing the *International Code of Conduct for Information Security*<sup>24</sup> to the UN General Assembly.

### 3. MODERNISING ARTICLE 17 ICCPR

In 1988, at the time when the General Comment No.16<sup>25</sup> on Article 17 ICCPR was adopted, the impact of advances in information and communication technologies on the right to privacy was barely understood, as the Internet was in its infancy. The paradigm shift in the way we communicate and the aggressive collection of personal information by many states have significantly undermined this right in recent decades. Consequently, there have been a number of calls for the Human Rights Committee (HRC) to draft a new general comment, most notably from UN Special Rapporteur Frank La Rue,<sup>26</sup> by the General Assembly,<sup>27</sup> and by civil society.<sup>28</sup> There are a number of reasons for updating General Comment No.16, and the fundamental starting point of this process must be articulating what the right to privacy actually

<sup>19</sup> Statement by H.E. Dilma Rousseff, President of the Federative Republic of Brazil at the Opening of the General Debate of the 68th Session of the United Nations General Assembly (24 September 2013).

<sup>20</sup> Ryan Gallagher, ‘After Snowden Leaks, Countries Want Digital Privacy Enshrined in Human Rights Treaty’, *Slate* (26 September 2013).

<sup>21</sup> 35th International Conference of Data Protection and Privacy Commissioners, Resolution on Anchoring Data Protection and the Protection of Privacy in International Law, (23-26 September 2013).

<sup>22</sup> UNHRC ‘Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci’ (8 March 2016) UN Doc A/HRC/31/64 para 46(j).

<sup>23</sup> *Ibid.*

<sup>24</sup> UNGA International Code of Conduct for Information Security (14 September 2011) UN Doc A/66/359; UNGA, ‘Letter Dated 9 January 2015 from the Permanent Representative of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General’ (2015) UN Doc A/69/723.

<sup>25</sup> 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.

<sup>26</sup> UNHRC (n 1).

<sup>27</sup> UNGA Res 68/167 (n 6).

<sup>28</sup> UNHRC ‘Written Statement by Reporters Without Borders International, a Non-Governmental Organisation in Special Consultative Status’ (4 September 2013) UN Doc A/HRC/24/NGO/31.

means and protects, together with the scope of extraterritorial obligations of states under the human rights treaties. Both of these aspects will be discussed in turn below.

### *A. The Meaning of Privacy*

The first step in modernising Article 17 must be the development of a better, more detailed and universal understanding of what is meant by ‘right to privacy’ in the 21st century.<sup>29</sup> The absence of a universally agreed and accepted definition, and the different rates of economic development and technology deployment in diverse geographical locations, mean that the principles relating to privacy that were established fifty years ago at the time of drafting the ICCPR need to be further developed and supplemented to make them more relevant and useful to the realities of the modern era.<sup>30</sup> The debate on the understanding of what privacy is and should be has only just begun. However, some aspects for discussion regarding this concept have been put forward by the Special Rapporteur Cannataci as a useful starting point. Several countries, including Brazil and Germany, have written into their constitutions an overarching fundamental right to dignity and to free, unhindered development of an individual’s personality.<sup>31</sup> Existing rights such as privacy, freedom of expression and freedom of access to information also constitute a tripod of enabling rights and, together with the fundamental right to dignity and the free and unhindered development of one’s personality, would help to articulate how the concept of privacy should be understood in the modern age.

The definition of privacy must also encompass the idea of autonomy and self-determination, which in some countries such as Germany gives rise to a constitutional right to ‘information self-determination’.<sup>32</sup> This idea is also referred to as ‘informational privacy’ and is concerned with the interest of individuals in exercising control over access to information about themselves.<sup>33</sup> This is in part already reflected in the current general comment to Article 17, according to which ‘the gathering and holding of personal information on computers, databanks and other devices by public authorities or private individuals or bodies, must be regulated by law’.<sup>34</sup> The Human Rights Committee has applied this framework in several of its Concluding Observations<sup>35</sup> and this practice is also present in the jurisprudence of the European Court of Human Rights (ECtHR). The Court has held that the notion of ‘private life’ is ‘not susceptible to exhaustive definition’<sup>36</sup> and has found on numerous occasions that ‘protection of personal data is of fundamental importance to a person’s enjoyment of respect for his or her personal data and family life’.<sup>37</sup> Article 8 of the Charter of Fundamental Rights of the European Union, explicitly recognises the right to protection of personal data separately and in addition to the right to privacy under Article 7.<sup>38</sup> In this regard, the Court of Justice of the European Union (CJEU) delivered a landmark decision in *Schrems v Data Protection Commissioner*,<sup>39</sup> holding

<sup>29</sup> UNHRC (n 22), para 46(a).

<sup>30</sup> *Ibid.*

<sup>31</sup> *Id.*, para 25.

<sup>32</sup> *Ibid.*

<sup>33</sup> American Civil Liberties Union, ‘Information Privacy in the Digital Age’ (February 2015) <[https://www.aclu.org/files/assets/informational\\_privacy\\_in\\_the\\_digital\\_age\\_final.pdf](https://www.aclu.org/files/assets/informational_privacy_in_the_digital_age_final.pdf)>

<sup>34</sup> UNHRC (n 25), para 10.

<sup>35</sup> UNHRC ‘Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Spain’ (2009) UN Doc CCPR/C/ESP/CO/5, para 11.

<sup>36</sup> *Bensaid v the United Kingdom* (App No 44599/98) (2001) ECHR para 47; *Botta v Italy* (App No 21439/93) (1994) ECHR.

<sup>37</sup> *MK v France* (App No 19522/09) (2013) ECHR; *S and Marper v the United Kingdom* [GC] (App Nos 30542/04 and 30566/04) (2008) ECHR.

<sup>38</sup> Charter of Fundamental Rights of the European Union, arts. 7 and 8, 2000/C 364/01 (12 December 2000).

<sup>39</sup> *Maximilian Schrems v Data Protection Commissioner* (6 October 2015) Case C-362/14.

that ‘legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental rights guaranteed by Article 7 of the Charter’.<sup>40</sup>

A new general comment should therefore affirm that Article 17 applies to informational privacy, which is understood as the individual’s right to access and control personal data.

### *B. Extraterritorial Application of Human Rights Treaties*

Governments may and do carry out surveillance both within and beyond their borders. However, the extent of the mass surveillance abroad, together with the international cooperation and the intelligence sharing among the Five Eyes partners, raises questions regarding these states’ extraterritorial obligations under international law.

The jurisdictional scope of the ICCPR is set out in Article 2(1) of the Treaty and obliges member states ‘to respect and to ensure’ the rights recognised in the treaty ‘to all individuals within its territory and subject to its jurisdiction’.<sup>41</sup> Similarly, Article 1 of the ECHR provides that state parties must secure to everyone within their jurisdiction the Convention’s rights and freedoms.<sup>42</sup> The legislative frameworks, pursuant to which global surveillance of the Five Eyes operates, make a distinction between external and internal communications (e.g. UK Regulation of Investigatory Powers Act 2000 (RIPA)),<sup>43</sup> and the communications of nationals and non-nationals.<sup>44</sup> These laws differentiate between the obligations owed to nationals and those within the state’s territory, and non-nationals who are outside state borders. For example, under ss.8 (1) and (2) RIPA, ‘internal’ communications may only be intercepted under a warrant which relates to a specific individual or address and may be granted on the basis of a suspicion of unlawful activity.<sup>45</sup> In cases of interception of ‘external communications’, defined as ‘means of communication sent or received outside the British Islands’,<sup>46</sup> ss.8(1) and (2) do not apply, which means that there is no need to identify any particular person who is to be the subject of the interception, or a particular address that will be targeted. The definition of ‘external’ communications, by the UK government’s own admission, seems to encompass all activities of UK residents conducted through such platforms as Facebook, Twitter and Google, as their headquarters are located in the US.<sup>47</sup> This gives the UK intelligence agencies *carte blanche* to intercept all communications in and out of the UK, and means that UK residents are being deprived of the essential safeguards that would otherwise apply to them. Consequently, both UK residents’ and foreigners’ communications may be monitored indiscriminately under a ‘general warrant’ on the basis of s.8(4) RIPA 2000. The UN Human Rights Committee commented on this differentiation in its 2015 *Periodic Report on the United Kingdom*, stating that:

the Regulation of Investigatory Powers Act 2000 (RIPA), that makes a distinction between ‘internal’ and ‘external’ communications, provides for untargeted warrants

<sup>40</sup> Id., para 94.

<sup>41</sup> ICCPR (n 4), art 2(1).

<sup>42</sup> ECHR, (n 5), art 1.

<sup>43</sup> UK Regulation of Investigatory Powers Act 2000 s.8(4); Investigatory Powers Act 2016 s 136(3); New Zealand Government Security Bureau Act 2003 s.15A.

<sup>44</sup> US Foreign Intelligence Surveillance Act 1978 s 1881a(a); Australian Intelligence Services Act 2001 s 9; Canadian National Defence Act 1985 s 273.64(1).

<sup>45</sup> RIPA, (n 43), s 8(2).

<sup>46</sup> Id., s 20.

<sup>47</sup> *Privacy International v GCHQ*, Witness Statement of Charles Blandford Farr on Behalf of the Respondent (16 May 2014) IPT/13/92/CH.

for the interception of external private communications and communication data, which are sent or received outside the United Kingdom without affording the same safeguards as in the case of interception of internal communications.<sup>48</sup>

The HRC urged the UK to:

review the regime regulating the interception of personal communications and retention of communications data ... with the view to ensuring that such activities both within and outside the State party, conform to its obligations under the [International Covenant of Civil and Political Rights], including Article 17.<sup>49</sup>

Despite this recommendation, the new Investigatory Powers Act 2016 s.136(3) which seeks to reform the regime under which the UK law enforcement and security agencies perform their functions, allows that bulk interception warrants be issued to collect 'overseas related communications'.<sup>50</sup>

The issue of the extent of the human rights obligations of states' intelligence agencies conducting surveillance in cyberspace remains far from settled. The US government has consistently denied that it is bound by its obligations under the ICCPR, which the US ratified in 1992, with respect of acts done outside its physical territory.<sup>51</sup> It is therefore not legally bound to comply with the ICCPR in relation to its surveillance over non-US communications, or Internet activities. The US government's position is that the Covenant obligations are restricted to situations when a person is both within a state's territory *and* subject to its jurisdiction.<sup>52</sup> This means that foreigners who do not satisfy both those conditions simultaneously do not benefit from the protection of the ICCPR.<sup>53</sup>

In the context of the UK state cyber surveillance, the Investigatory Powers Tribunal (IPT), which oversees the working methods of the intelligence agencies, has recently considered the issue of the extraterritorial human right obligations of the UK in *Human Rights Watch and Others v The Secretary of State for the Foreign and Commonwealth Office and Others (HRW v Secretary of State)*.<sup>54</sup> The case related to the interception, storage and use of information and communications by GCHQ of two groups of applicants – those resident in the UK and those who are not. Regarding the latter, the IPT ruled that the UK:

owes no obligation under Article 8 ECHR to persons [who] are situated outside its territory in respect of electronic communications between them, which pass through that state.<sup>55</sup>


48 UNHRC 'Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland' (17 August 2015) UN Doc CCPR/C/GBR/CO/7.

49 Ibid.

50 RIPA (n 43).

51 UNHRC 'Summary Record of the 1405th Meeting' (24 April 1995) UN Doc CCPR/C/SR.1405, para 20; UNHRC 'Consolidation of Reports Submitted by States Parties under Article 40 of the Covenant' (2005) UN Doc CCPR/C/USA/3.

52 Id., para 20.

53 US Department of State 'Second and Third Periodic Report of the United States of American to the UN Committee on Human Rights Concerning the International Covenant on Civil and Political Rights' (October 2005), Annex I. 

54 *Human Rights Watch Inc. and Others v The Secretary of State for the Foreign and Commonwealth Office and Others* [2016] ALL ER (D) 105 (May).

55 Id., [60].



The IPT reasoned that foreigners not physically present in the UK, but subject to GCHQ surveillance under s.8(4) RIPA, do not have a right to privacy under Article 8 ECHR because they have not enjoyed a private life in the UK and therefore under Article 1 ECHR the UK is under no obligation to respect it.<sup>56</sup> In rejecting the extraterritorial application of the ECHR, the IPT adopted a conservative approach, based on *Bankovic v Belgium*<sup>57</sup> whereby, as a general principle of international law, jurisdictional competence of states is primarily territorial. The IPT was thus unwilling to ‘extend the bounds of the UK Courts’ jurisdiction under Art 8’.<sup>58</sup>

Ultimately, the issue of UK mass cyber surveillance abroad will be for the ECtHR to resolve in this and other cases.<sup>59</sup> Nonetheless, *HRW v Secretary of State* and the US consistent rejection of the extraterritorial application of the ICCPR obligations highlight the acute lack of transnational legislative instruments capable of addressing this issue. Suggestions have been made, however, that the ‘effective control’ over digital communications infrastructure, discussed in more detail below, may give rise to states’ human rights obligations.<sup>60</sup>

### *C. Models of Extraterritorial Application of the ICCPR and the ECHR*

The jurisdictional competence of a state is primarily territorial.<sup>61</sup> However, all major human rights courts and bodies, including the International Court of Justice (ICJ), the UN HRC, the Inter-American Commission on Human Rights (IACHR) and the ECtHR, agree that in some circumstances human right obligations may apply extraterritorially. This means that a state is bound by international human rights law in relation to individuals who may be not within its borders, but who are under its jurisdiction. To that end, a broadly similar approach, based on ‘effective control’, has been adopted to determine jurisdiction. Thus, the HRC has held that:

a State Party must respect and ensure the rights laid down in the [International] Covenant [of Civil and Political Rights] to anyone within the power, or effective control of that State Party, even if not situated within the territory of the State Party.<sup>62</sup>

Similarly, the IACHR has established that, to determine whether a person is within a state’s jurisdiction or not:

the inquiry turns not on the presumed victim’s nationality, or presence within a particular geographical area, but on whether under specific circumstances, the State observed the rights of a person subject to its authority and control.<sup>63</sup>

In conceptualising when and how the international human rights obligations may arise outside a state’s territory, two types of extraterritorial jurisdiction were distinguished, namely the spatial and the personal models. The spatial model sees jurisdiction as effective overall control over a geographical area, whereas the personal sees it as a physical control over an individual. The

<sup>56</sup> Id. [58].

<sup>57</sup> *Bankovic and Others v Belgium* (App No 52207/99) (2007) 44 EHRR, 57.

<sup>58</sup> *HRW v Secretary of State* (n 54), [58].

<sup>59</sup> *Big Brother Watch v the United Kingdom* (App No 58170/13); *10 Human Rights Organisations v the United Kingdom* (Index No IOR 60/1415/2015); *Bureau of Investigative Journalism and Alice Ross v the United Kingdom* (App No 62322/14).

<sup>60</sup> OHCHR (n 3), para 34; Emmerson (n 7), para 41.

<sup>61</sup> *Bankovic* (n 57).

<sup>62</sup> UNHRC ‘General Comment No. 31. The Nature of the General Obligations Imposed on State Parties to the Covenant’ (2004) UN Doc CCPR/C/21/Rev.1/Add1326 May 2004, para 10.

<sup>63</sup> *Alexandre v Cuba*, Case 11.589, (1999) IACHR Report No. 109/99, para 37.



spatial model was articulated by the ECtHR in *Loizidou v Turkey*,<sup>64</sup> where the Court held that a state's responsibility was engaged when, as a consequence of lawful or unlawful military action, it exercised effective control of an area outside its national territory. A similar approach was adopted by the ICJ in the *Wall Advisory Opinion*<sup>65</sup> and in *DRC v Uganda*,<sup>66</sup> where it was held that the ICCPR applies extraterritorially when a state is occupying territory of another state. Whilst the spatial model has its merits, particularly in its clarity and in setting some limits on states' obligations, it also has some drawbacks.<sup>67</sup> According to Milanovic, 'a state is perfectly capable of violating the rights of individuals without controlling the actual area', for example by using drones for targeted killing thus dispensing with the need to have troops on the ground.<sup>68</sup>

The jurisprudence of the international human rights courts has also recognised that states have human rights obligations when exercising physical control over an individual. In *Lopez Burgos v Uruguay*<sup>69</sup> the HRC held that state parties are liable for the actions of their agents on foreign territory, as it would be

unconscionable to so interpret the responsibility under Article 2 of the [ICCPR] as to permit a State party to perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory.<sup>70</sup>

In its General Comment No.31, the Committee established that:

a State Party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party...regardless of the circumstances in which such power or effective control was obtained.<sup>71</sup>

However, by far the most varied jurisprudence regarding the personal model is that of the ECtHR. In *Al-Skeini v UK*<sup>72</sup> the Court stressed the primarily territorial nature of jurisdiction under the ECHR, but recognised exceptions to that principle, namely where state agents exercise authority and control extra-territorially, and when a state exercises effective control of an area outside national territory. State agent authority is particularly pertinent in military operations where physical authority and control is exercised in formal detention centres, as was the case in the British-controlled facilities in *Al-Skeini*. However, the exercise of authority was also held to have occurred outwith a formal detention centre in *Öcalan v Turkey*.<sup>73</sup> The case concerned the handover in Kenya to Turkish authorities of an individual suspected in Turkey of terrorist-related crimes. The ECtHR noted that he was effectively under Turkish authority and

<sup>64</sup> *Loizidou v Turkey* (App No 15318/89) (1995) 20 EHRR 99.

<sup>65</sup> Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories (Advisory Opinion) (2004) ICJ Reports 163.

<sup>66</sup> *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo v Uruguay)* (2000) ICJ Reports 111.

<sup>67</sup> Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal 81, 114-115.

<sup>68</sup> *Id.*, 113.

<sup>69</sup> UNHRC *Lopez Burgos v Uruguay*, Communications No 52/1979 (17 July 1979) UN Doc CCPR/C/13/D/52/1979.

<sup>70</sup> *Id.*, paras 12.2-12.3.

<sup>71</sup> UNHRC (n 62), para 10.

<sup>72</sup> *Al-Skeini and Others v United Kingdom* [GC] (App No 55721/07) (7 July 2011) ECHR 2011.

<sup>73</sup> *Öcalan v Turkey* (App No 46221/99) (2003) 41 EHRR 985.

therefore within its jurisdiction, even though Turkish officials at the time of the arrest exercised their authority outside Turkey.

In addition, and perhaps most notably, the ECtHR has recognised that the extraterritorial jurisdiction on the basis of state agent authority or control is not limited to situations of the physical custody of an individual, but may be engaged when state agents exercise authority and control over an individual's rights, as was the case in *Jaloud v the Netherlands*.<sup>74</sup> The case concerned the fatal shooting of Azhar Sabah Jaloud, who at the time was passing through a checkpoint manned by personnel under the command and direct supervision of a Royal Netherlands Army officer in Iraq. The ECtHR found that the Netherlands exercised its jurisdiction on the basis that Dutch troops asserted 'authority and control over persons passing through the checkpoint' because they exercised authority and control over his right to life at that moment. This gave rise to extraterritorial jurisdiction, despite not having physical control over Mr Jaloud. The case therefore marks the ECtHR moving away from an approach wherein jurisdiction is founded on the basis of pure factual authority, towards one based on the exercising of authority and control over an individual's rights.

#### *D. Applicability of Human Rights Treaties to Extraterritorial Cyber Surveillance*

If a state may be found to have human rights obligations because it exercises authority and control over an individual's right to life, as proposed in *Jaloud*, then by analogy the exercise of control over their right to privacy of communications should also give rise to extraterritorial obligations in cases of foreign cyber surveillance. Such an interpretation seems necessary, given that the 'effective control' test is unsuitable, outdated and narrow in the context of state-sponsored cyber surveillance operations. It is outdated, because it has been articulated by international human rights courts and bodies long before digital technologies begun to play such a pervasive role in the lives of millions of individuals around the world. The existing approach is entirely inadequate for the cyber and communications realm, as it places the emphasis on the exercise of physical control over persons or territory, which is difficult to relate to cyberspace.<sup>75</sup> The shortcomings of the effective control approach centre around the fact that some state intelligence services, particularly the NSA, exert effective remote, rather than physical, control over much of the communications of foreign nationals abroad.<sup>76</sup> This occurs through eavesdropping on those communications, filtering, or altering their content, and breaking many forms of encryption by installing 'back doors' in many software systems.<sup>77</sup> The NSA also has the capacity to gain control of computers not directly connected to the Internet due to implantation of transmitting devices in computers manufactured in the US and elsewhere.<sup>78</sup> In addition, the US has relationships with Internet and telecommunications companies that facilitate surveillance, and therefore have the capacity to access directly the undersea cables and other carriers of Internet and telephonic communications.<sup>79</sup> The US's virtual power is unprecedented,<sup>80</sup> and the narrowly defined standard requiring physical control means that states interfering with the right to privacy would continue to exploit this gap by circumventing their

<sup>74</sup> *Jaloud v the Netherlands* (App No 47708/08) (2014).

<sup>75</sup> Peter Margulies, 'The NSA in the Global Perspective: Surveillance, Human Rights and International Counterterrorism' (2014) 82 *Fordham Law Review* 2137.

<sup>76</sup> *Id.*, 2151.

<sup>77</sup> *Ibid.*

<sup>78</sup> *Ibid.*

<sup>79</sup> *Ibid.*

<sup>80</sup> *Ibid.*

human rights obligations. There can be no doubt, therefore, that the ‘effective control’ test must be adapted to suit the realities of cyber surveillance operations.

A number of suggestions have been made, and their overall tenet seems to hinge on the control of communications, rather than physical control over areas or individuals. Thus, Nyst argues that when data or communications are intercepted within a state’s territory, the state should owe obligations to those individuals regardless of their location on the basis of ‘interface-based jurisdiction’,<sup>81</sup> that is not to interfere with communications that pass through its territorial borders.<sup>82</sup> This approach is broadly in line with that proposed by Milanovic, who distinguishes between the overarching positive obligation of states to secure or ensure human rights, and extends even to preventing human rights violations by third parties and negative obligations of states to respect human rights that only requires states to refrain from interfering with the rights of individuals without sufficient justification.<sup>83</sup> This model conceptualises jurisdiction as a negative duty to refrain from interference and would apply to all potential violations of negative obligations, for example to refrain from interfering with privacy.<sup>84</sup> In this sense, human rights treaties would apply to most, if not all foreign surveillance activities.<sup>85</sup> Both these approaches have their merits, in as much as they recognise the weaknesses of the personal and spatial models and emphasise the negative duty of states not to interfere with protected rights. However, the nature and scope of the Five Eyes surveillance seems to go beyond the interception, collection and storage of data. The partnership between the US and its allied services allows governments to easily engage in the so-called ‘collusion for circumvention’.<sup>86</sup> For example, GCHQ is allowed to spy on anyone except British nationals, whilst the NSA on anyone but Americans.<sup>87</sup> Information-sharing partnerships enable each agency to circumvent its respective national restrictions protecting their countries’ citizens, since they are able to access the data collected by others.<sup>88</sup> This reciprocity has important ramifications on the domestic level if it is used to circumvent domestic legislation and limits on the governments’ ability to tap its own citizens’ communications.<sup>89</sup> In this context, the negative duty not to interfere with privacy would only be discharged if the interference is also understood as ‘collusion for circumvention’, encompassing such information sharing arrangements.

Given that this is not entirely clear, a sound candidate for a model of jurisdiction may be the ‘virtual control’ test, proposed by Margulies.<sup>90</sup> This test would make the ICCPR and other human rights treaties applicable when a state can assert ‘virtual control’ over an individual’s communications, even though it lacks control over the territory in which the individual is located, or over the ‘physical person’ of that individual.<sup>91</sup> ‘Virtual control’ in this context means the ability to intercept, store, analyse and use communications. Although it could be argued that mere surveillance does not constitute physical control, it may constitute virtual control, in that it

81 Carly Nyst, ‘Interface Based Jurisdiction Over Violations of the Right to Privacy’ (21 November 2013) EJIL:Talk! <<http://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/>>

82 Ibid.

83 Milanovic (n 67), 126.

84 Ibid.

85 Id., 129.

86 Parliamentary Assembly of the Council of Europe, ‘Mass Surveillance’ Doc 13734 (18 March 2015), paras 30-3.

87 Ibid.

88 Ibid.

89 Ibid.

90 Margulies (n 75), 2139.

91 Ibid.

not only stifles their right to privacy, but also has a chilling effect on other human rights, such as free expression, freedom of conscience and religion, free assembly and association, and health, to name but a few. It therefore affects and controls individuals' behaviour.

Although the 'virtual control' approach has been criticised for being new and 'without support in patterns of generally shared legal expectations about personal jurisdiction',<sup>92</sup> it has a number of advantages. First, it corresponds to the notion of control developed and required by human rights courts and bodies,<sup>93</sup> outlined above. Secondly, it responds to the jurisdictional challenges of human rights obligations in surveillance cases, because the intelligence agencies under scrutiny are perfectly capable of controlling lives and private information with the press of the button.<sup>94</sup> Thirdly, it is in line with the ECtHR reasoning in *Jaloud v the Netherlands*, where a more expansive approach was taken and extraterritorial jurisdiction was established because of the state agents' exercise of authority and control over the individual's right to life, which made their physical proximity unimportant. Fourthly, such an approach would ensure equal treatment of all individuals, irrespective of their nationality or physical location, because establishing 'virtual control' over someone's communications would not depend on where the interference takes place, but rather on whether or not a state can assert such control even when it lacks authority or control over the territory or the physical person. Finally, it could also mean that governments' 'collusion for circumvention' arrangements may fall within their obligations not to interfere with the privacy rights, as they would have an obligation derived from the human rights treaties in relation to the rights of all individuals whose communications fall within their control, either inside and outside their territories.

It still remains unclear how cyber surveillance may trigger the extraterritorial application of human rights law. Although there is a general endorsement from international organisations that human rights treaties apply to extraterritorial cyber surveillance, no human rights body has yet directly addressed how electronic surveillance affects the right to privacy in detail. The Human Rights Committee has engaged with this issue, suggesting that extraterritorial surveillance does affect the ICCPR, when addressing the NSA surveillance pursuant to s.702 of FISA, stating that:

the Committee is concerned about the surveillance of communications in the interest of protecting national security conducted by the National Security Agency (NSA) conducted both within and outside the United States.<sup>95</sup>

The United Nations Office of the High Commissioner also addressed extraterritorial surveillance noting that:

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

<sup>92</sup> Jordan J. Paust, 'Can You Hear Me Now? Private Communications, National Security and the Human Rights Disconnect' (2015) 15(2) *Chicago Journal of International Law* 612(2015), 625.

<sup>93</sup> Ilina Georgieva, 'The Right to Privacy under Fire-Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR' (2015) 31(80) *Utrecht Journal of International and European Law* 104.

<sup>94</sup> *Ibid.*

<sup>95</sup> UNHRC, 'Concluding Observations on the Fourth Periodic Report of the United States of America' (April 2014) CCPR/C/USA/CO/4, para 22.



direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant.<sup>96</sup>

Similarly, the Special Rapporteur Emmerson observed that the:

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.<sup>97</sup>

The United Nations General Assembly, in adopting Resolution 68/167, appears to support the view that the ICCPR applies to extraterritorial surveillance, expressing its deep concern:

at the negative impact that surveillance [...] including extraterritorial surveillance [...] in particular when carried out on a mass scale may have on the exercise and enjoyment of human rights.<sup>98</sup>

These approaches seem to broadly correspond with legal academic opinion articulating jurisdiction being triggered on the basis of states' control over the individual's rights to privacy. However, they leave unanswered the question of what degree of control is necessary to establish that a state exercises 'power or effective control in relation to digital communications infrastructure'. In *Jaloud* the ECtHR indicated its approach to the issues of authority and control based on the actual exercise of such powers over an individual's rights. Whether or not it will apply this or a similar approach to the pending surveillance cases<sup>99</sup> remains to be seen.

There can be no doubt that, as currently defined, the 'effective control' test of extraterritorial jurisdiction is not well suited for application to cyber surveillance operations. Cyberspace is a transnational environment where information is deliberately routed through a number of jurisdictions to reach its destination. When interference is conducted remotely, physical control over an area or an individual ceases to be relevant. At the very least, it leaves a gap that intelligence agencies can exploit to circumvent the obligations under the human rights treaties through the use of intelligence sharing agreements. What becomes important in this context is the 'virtual control' over the individuals' right to privacy, regardless of where they are located or their nationality. How these obligations may apply to cases of cyber surveillance remains unclear, especially bearing in mind the 'inevitable ripple effects on other scenarios such as extraterritorial use of lethal force through, for example drone strikes',<sup>100</sup> if more permissive approach to this issue were to be adopted. This makes the task of the Human Rights Committee when drafting new general comment on Article 17 particularly challenging.

<sup>96</sup> OHCHR (n 3), para 34.

<sup>97</sup> Emmerson (n 7), para 41.

<sup>98</sup> UNGA Res 68/167 (n 6).

<sup>99</sup> Listed at note 59.

<sup>100</sup> Marko Milanovic 'UK Investigatory Powers Tribunal Rules that Non-UK Residents Have No Right to Privacy under the ECHR' (2016) EJIL: Talk!

## 4. CONCLUSION

In the age of increased terrorist threat, the balance between the need for security and the right to privacy of innocent individuals is particularly difficult to achieve. The vulnerability of this and other rights in the face of an unprecedented interference by states' intelligence agencies conducting mass surveillance must be addressed. This paper concentrated on one legal solution – the overhaul of Article 17 ICCPR, and in particular re-defining the concept of privacy and addressing the question of how and when states may be liable under international law for their surveillance activities, the effect of which may be felt beyond their borders. The paper has illustrated that the narrowly defined territorial limitations on human rights protection based on nationality (e.g. s.702 FISA), or geographical distinctions (s 8(4) RIPA; s.136 IPA) are meaningless when applied to highly integrated global communications networks. The surveillance conducted on these legal bases, coupled with the states' 'collusion for circumvention' places practically no limitation on the extent to which governments can access the communications of millions of individuals in their own and other countries. Yet the enjoyment of fundamental rights is not limited to citizens of particular states, but includes all individuals, regardless of nationality. Although the jurisprudence of the international human rights courts recognises that there are certain circumstances when extraterritorial human rights obligations will be engaged based on the 'effective control' test, this paper has highlighted its limitations in the context of cyber surveillance and has proposed that the 'virtual control' test – understood as a remote control over an individual's right to privacy – may be a solution to this problem.