UTRECHT JOURNAL OF
INTERNATIONAL AND EUROPEAN LAW

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, DOI: http://dx.doi.org/10.5334/ujiel.cr

RESEARCH ARTICLE

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

Ilina Georgieva[1]

[1] Senior Research Associate at the Public International Law & Policy Group (PILPG), the Netherlands
ilina_georgieva@hotmail.com

The recent exposure of the NSA documents has raised a great deal of concerns with regards to the effective control of companies that cooperate with intelligence agencies. It also exposed a network of secret government spying partnerships used to go around existing domestic guarantees and to spy on one's own citizens through the back door. The dread that both legal and technological means designed with legitimate purposes such as counter-terrorism and crime prevention are also employed for total social control is now out there. In many aspects it looks like we are experiencing the end of privacy and opting for a 'surveillance society' instead. In the clutter of pressing issues, most of the recent scholarly attention has focused on the assessment and reform proposals of the existing, but as it turns out inadequate with respect to actual rights protection, domestic legal frameworks. This has left the obligations of the intruders under international human rights law unconsidered. Therefore, the present paper aims at evaluating the legality of such surveillance programs under the International Covenant on Civil and Political Rights and the European Convention on Human Rights.

Keywords: NSA; Privacy; Foreign Surveillance; International Security; Counter-terrorism; Human Rights

I. Introduction

A. The Surveillance Context

Privacy is multifaceted, subjective, and evolving.[1] It concerns every single human being in his or her most personal and private matters. It is a fundamental human right that, due to contemporary technological developments, is almost constantly in the line of fire. Over the last decade, law in Europe and the US has managed to strengthen the ability of public authorities to obtain communications data at the expense of privacy.[2] Thus, the intensification of the debate on the protection of privacy as a human right is not a novel one and has constantly surfaced in the discussions of politicians, practitioners, academics and activists. Legal scholarship has focused especially on the justification of privacy intrusions, which are often vested in terms of public safety and how the protection of public safety demands the narrowing of privacy protections.[3]

Yet, ever since Edward Snowden's revelations on the US National Security Agency's ('NSA') activities in the summer of 2013, privacy questions have become an integral part of the international agenda, turning individuals' data protection into a serious global issue.[4] Information on surveillance that has been intentionally kept in the dark is now a matter of heated public debate mostly because the leaked documents

[1] Zhendong Ma and others, 'Towards a Multidisciplinary Framework to Include Privacy in the Design of Video Surveillance Systems' in *Privacy Technologies and Policy*, Springer 2014, 103

[2] Joel R. Reidenberg, 'The Data Surveillance State in the United States and Europe' (2013) Wake Forest Law Review, Forthcoming, <http://ssrn.com/abstract=2349269> p. 2

[3] ibid

[4] Stephanie Schiedermair, 'Data Protection – Is There a Bridge across the Atlantic?' in Dieter Dörr and Russell L. Weaver (eds), *The Right to Privacy in the Light of Media Convergence Perspectives from Three Continents* (De Gruyter 2012) 17

confirmed something the international community has long suspected and feared.[5] However, it was the extent of the exposed surveillance program that led to reconsiderations of current policies and technologies. Citizens now fear that both legal and technological means designed with legitimate purposes, such as counter-terrorism and crime control, are also increasingly used for total social control.[6] In many aspects it looks like we are experiencing the end of privacy and evolving to a 'surveillance society' instead. However, do the ends justify the means?[7]

The NSA is the world's largest surveillance organisation, which has been able to conduct its activities together with the national intelligence agencies of 'second parties' (UK, Australia, Canada and New Zealand) for more than a decade.[8] Among the 'second party' countries, also commonly referred to as the Five Eyes, the performance of UK's Government Communications Headquarters ('GCHQ'), which is Her Majesty's (HM) primary agency for the undertaking of Internet surveillance, has been crucial for the expansion of the surveillance framework abroad.

The classified documents leaked to the press demonstrate that the US-UK surveillance ensemble has not only targeted foreign governments and international institutions like the EU, the International Atomic Energy Agency (IAEA) and the UN systematically and on regular bases, but also that citizens around the globe have been monitored extensively for quite some time now.[9] In the process, no independent institutional control has been exercised over the activities of the respective agencies.

In the clutter of pressing issues that need attention, it is rather surprising that, except for the UN General Assembly resolution on the right to privacy from the 18th of December 2013,[10] which was followed by a couple of discussions and proposals,[11] most of the scholarly attention has been focusing on the assessment and reform proposals of the existing, but as it turns out inadequate with respect to actual rights protection, domestic legal frameworks. This has left the obligations of the intruders under International Human Rights Law ('IHRL') quite under-considered. The latter discovery leads us to the purpose of the present paper – it aims at offering assistance in closing this gap by providing an extensive evaluation of the legality of such surveillance programs under the International Covenant on Civil and Political Rights[12] ('ICCPR') and the European Convention on Human Rights[13] ('ECHR'), both of which protect extensively the right to privacy (Art. 17 ICCPR and Art. 8 ECHR). Most countries engaged in and affected by foreign surveillance activities are parties to the ICCPR, which renders the analysis of its provisions crucial. The ECHR, a regional framework, deserves attention because it imposes binding human rights obligations on the British government in categorical terms. Owing to the active role of the European Court of Human Rights (ECtHR), the framework of the ECHR is one of the most developed in terms of human rights protection. Thus it is often referenced and serves as an example in the proceedings before other human rights bodies. Further, the ECHR is of importance because some of the affected states in Europe (for example, Germany) are bound by its regulations too.

The specific example of the NSA/GCHQ activities affords us an opportunity to conceptualize the present paper as a case study. It includes in the first place a theoretical analysis and discussion of selected approaches to the territorial applicability of the two major human rights treaties in order to illustrate the useful concepts that allow for an adequate application of human rights norms to surveillance conducted by a state outside its borders. The investigation continues with the evaluation of the privacy interests at stake. Here, the case study follows notionally the examination steps as established by the Human Rights Committee ('HRC') and the European Court of Human Rights.[14] In the assessment of the specific legal requirements of Art. 8 ECHR

---

[5] Cf. Monica Ermert, 'Mass Surveillance No Surprise to Many in Technology and Politics' (*Intellectual Property Watch*, 12 June 2013) <http://www.ip-watch.org/2013/06/12/mass-surveillance-no-surprise-to-many-in-technology-and-politics/>

[6] Elisabeth Fura and Mark Klamberg, 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA' in *Freedom of Expression: Essays in honour of Nicolas Bratza,* President of the European Court of Human Rights 2012, 463

[7] ibid

[8] This is an internal NSA document's description for the US's closest allies UK, Australia, Canada and New Zealand, cf. Laura Poitras and others, 'How the NSA targets Germany and Europe' (*Spiegel Online International*) <http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html>

[9] Laura Poitras and others, 'Codename 'Apalachee': How America Spies on Europe and the UN' (*Spiegel Online International*) <http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html>

[10] UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167

[11] Cf. Human Rights Council, 'Panel Discussion on the Right to Privacy in the Digital Age' (24 March 2014) A/HRC/25/L.12

[12] International Covenant on Civil and Political Rights (adopted16 December 1966, entered into force 23 March 1976) 999 UNT 171 (ICCPR)

[13] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended)

[14] Cf. Marco Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2014) HILJ <http://ssrn.com/abstract= 2418485> 68 forthcoming

and Art. 17 ICCPR, a crucial part of the present contribution is devoted to the related jurisprudence of the ECtHR and the HRC. This approach has as an objective to outline the already existing data and privacy 'protection culture' on each side of the Atlantic.[15] This is necessary in order to establish the applicable standards for the evaluation of new surveillance technologies and their impact on individual privacy interests. The deduced guidelines shall be then considered in the specific example of the NSA/GCHQ surveillance activities. In the comprehensively addressed cases,[16] special attention shall be given to the ECtHR's judgements, which have already dealt with and evaluated the use of new information exchange methods when personal data is of interest to others. The cases of e.g. *Klass and others v Germany*, *Malone v United Kingdom* and *Weber and Saravia v Germany* provide valuable insight into the ECtHR's reasoning and proceedings when addressing national laws, directives and practices that have allowed surveillance measures in the first place.

This article will address a certain interrelation between the positions of the ECtHR and the HRC. This interesting fact is at once the evidence of the ever increasingly-linked human rights frameworks around the globe. Thanks to the progressive work of the human rights bodies instructed with the tasks of guarding and interpreting the respective treaties, we are able to witness how the notion of universality blossoms out to formal, legal universality too.

Borrowing Milanovic's idea[17] for the purpose of convenience, I shall use the term 'foreign surveillance' as a generic description of a wide range of activities. That is to say, where an activity referred to is not precisely specified, foreign surveillance would encompass data collection and storage practices, processing and transfer of the gathered data to a third party, but also interception of electronic or other kinds of communications.

The present work is divided in three parts. After this introduction, part one continues by illustrating in more detail the problematic surveillance practices of the NSA and the GCHQ. Part two analyses the legality of the NSA/GCHQ activities conducted abroad, looking first into the applicability of the ECHR and the ICCPR outside of national borders. For this purpose this article = considers the developments in the human rights bodies' jurisprudence before and after the case of *Bankovic.*[18] This article then applies Art. 8 ECHR and Art. 17 ICCPR to the surveillance programs in question, taking into consideration the existing case-law on privacy interferences developed by the HRC and the ECtHR in the surveillance cases they have so far dealt with. Part three draws the attention of the reader to the most pressing protection concerns and provides suggestions for strengthening the existing privacy safeguards. It is then followed by the conclusion of the present investigation.

B. Foreign Surveillance Activities under Scrutiny

The following section illustrates briefly the major press revelations that provide us with the relevant information on foreign surveillance[19] methods and activities that later shall be placed under the magnifying glass. However, before turning to more details, it should be also noted that all the information is based on recent disclosures. While with regard to the NSA activities this is rather unproblematic, for the media reports were usually accompanied by authentic leaked documents and Snowden revealed himself as the source of the leaks soon, most of the information on the GCHQ has been provided by anonymous sources. Up until now there was almost no other information regarding the GCHQ's practices, which makes it difficult to assess the credibility of the claims. Further, the concerned transaction types are not only expansive, but leave no trace in the communication systems, which makes them more difficult to detect and put on record. However, the Guardian reports on the subject appear to be credible. Some of the information in the published leaks has been confirmed by government officials, and by earlier disclosers (including assertions by the former senior NSA official William Binney).[20] As to the technical equipment for such surveillance operations, there is no doubt that the necessary technology is available on the market. Thus, the issue of the statements' reliability regarding the British agency will not be further broached. In the following, some of the core surveillance programs will be introduced.

---

[15] Schiedermair (n 4) 358

[16] See below esp. sections II. C and II. D

[17] Cf. Milanovic (n 16) 7

[18] *Bankovic et al. v. 17 NATO Member States* App no. 52207/99 (ECtHR, 12 December 2001)

[19] As indicated above under I. A on p. 4, foreign surveillance is used as a generic term for describing all surveillance activities that cross national borders and thus concern the privacy rights of foreign citizens

[20] Cf. Ian Brown, 'Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK' (2013), Application No. 58170/13 to the European Court of Human Rights <http://ssrn.com/abstract=2336609> 17

Some NSA program tools e.g. 'Boundless Informant' record specific transactional data such as the time and date of a call, as well as its location. This type of information, also commonly referred to as metadata,[21] although not including the content of the messages and the personal information of the subscribers, allows for quantification and later tracking of the user based solely on an IP-address or a phone number.[22] Metadata is extremely useful when an intelligence agency wishes to reproduce the contact framework of a target. Alone in Germany as one of the revealed state targets, the US intelligence service each month saves data from around half a billion communications.[23] A further revelation was the US use of the 'Fairview' program which exposed foreign telecoms' partnerships with US telecoms that enable the NSA to gain access to Internet and telephone data of non-US citizens.

Yet another exposed program called 'PRISM' provides the NSA with direct access to the systems of Microsoft, Google, Facebook, Apple and many other US technology companies. The program is of a special value to the NSA intelligence activities, because it grants direct access to the servers of the private companies[24] and enables the collecting of data including search history, email content, the transfer of files and live chats.[25] It would appear that the Agency stores the captured data for about two years.[26] In addition, one can only fully imagine the magnitude of the NSA operations by bearing in mind that most of the internet administrators are located on US soil, which means that the agency is tapping directly into the world's internet backbone.[27]

Further, with regard to the UK activities, the report of 21 June 2013 published in the Guardian[28] disclosed the 'Tempora' program, which involves the placement of data interceptors by the GCHQ on fibre-optic cables conveying Internet data within and out of the UK. The cables located in the UK include transatlantic connections between the US and Europe. Much of the rest of Europe's external Internet traffic is routed through the UK, as this is the landing point for the majority of transatlantic fibre-optic cables. As a consequence, a large quantity of communications relating to the rest of the world is being intercepted. According to the newspaper report, the quantity of data was 'equivalent to sending all the information in all the books in the British Library 192 times every 24 hours'.[29] Tempora has most likely given GCHQ the largest Internet access out of the 'Five Eyes' group of countries. The data flows from the cable probe along fibre-optic cables to the GCHQ's monitoring stations. There, the information is reportedly stored using GCHQ's Internet buffers. The thus-obtained massive amounts of Internet data are stored for up to 72 hours (for actual content) and thirty days (for metadata content). Afterwards, the data is searched for signals using keywords, which are identified together by the NSA and the GCHQ and amount to some 40,000 'selector' pointers. After the signals have been identified, the operatives take a closer look and examine the respective communications.

Both the NSA and the GCHQ benefit from the activities of the other. A great deal of the PRISM data is transferred to the GCHQ servers. Likewise, Tempora makes a 'unique contribution [...] to the NSA in providing insights into some of their highest priority targets' by giving the NSA 36% of all the raw information from intercepted computers.[30]

While contemplating this information, a rather inevitable question emerges: how exactly are these activities compatible with the HR obligations of the states conducting foreign surveillance? An answer is provided in the next section.

---

[21] Cf. Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily' *The Guardian (*6 June 2013) <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>

[22] Guardian US Interactive Team 'A Guardian Guide to Your Metadata' (12 June 2013) <http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000>; see also Alex Sinha, 'NSA Surveillance Since 9/11 and the Human Right to Privacy' (2013) 59 Loy. L. Rev. 895

[23] Laura Poitras and others (n 8)

[24] Cf. Glenn Greenwald and Ewen McAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others' *The Guardian* (June 7 2013) <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link>

[25] ibid

[26] Tom Burghardt, 'Documents Show Undersea Cable Firms Provide Surveillance Access to US Secret State' (*Global Research*, 18 July 2013) <http://www.globalresearch.ca/documents-show-undersea-cable-firms-provide-surveillance-access-to-us-secret-state/5343173>

[27] 'Inside TAO: Documents Reveal Top NSA Hacking Unit' (*Spiegel Online International*, 29 December 2013) <http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-onglobal-networks-a-940969-3.html>

[28] Ewen McAskill and others, 'GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications' *The Guardian* (21 June 2013) <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

[29] ibid

[30] Nick Hopkins and others, 'GCHQ: inside the top secret world of Britain's biggest spy agency' *The Guardian* (1 August 2013) <http://www.theguardian.com/world/interactive/2013/aug/01/gchq-spy-agency-nsa-edward-snowden>

II. Legality of the Foreign Surveillance under the ICCPR and the ECHR

This part of the contribution seeks to determine the legality of the foreign surveillance activities as employed by the intelligence agencies NSA and GCHQ. Before turning to the actual legal assessment, one needs to establish the limits of the applicable legal framework. As it would be illustrated in the following sub-sections, extraterritorial applicability of the human rights instruments in question is disputed, but not out-of-place in the surveillance context. A further difficulty is also introduced by the fact that the applicable test of how extraterritorial human rights obligations are triggered has been coupled with the notion of physical control over populations and territories. This is a rather unsuitable test for the NSA/GCHQ surveillance activities, which are conducted in cyberspace. Accordingly, the question of how this jurisdictional test could take place with regard to privacy intrusions in the cyber domain shall be discussed under A.2.c).

A. Applicability of the ECHR and the ICCPR to Foreign Surveillance Activities

As indicated above, in the foreign surveillance context – undoubtedly an activity crossing national borders – the provisions of the selected human rights instruments are coupled with the preliminary question of their extraterritorial application. Therefore, the following section shall examine the possibilities of applying the ICCPR and the ECHR where State parties deploy their monitoring activities outside of their national borders.

The research in the present section focuses in the first place on Art. 2 (1) ICCPR and Art. 1 ECHR. Both provisions refer to the 'jurisdiction'[31] of the respective States parties, although Art. 2 (1) ICCPR seems to couple the jurisdiction requirement with a further one of territorial nature by stipulating that Covenant's rights are to be guaranteed 'to all individuals within its territory and subject to its jurisdiction'.[32] This particular wording of Art. 2 (1) ICCPR is however highly relevant, for it might be understood as a categorical denial of any kind of extraterritorial application of the Covenant. Therefore, before illustrating in detail how the different human rights bodies have dealt with the notion of jurisdiction so far, a careful analysis of the territorial reference and its meaning for the scope of application of the ICCPR must be rendered. In order to achieve a plausible result this investigation shall, among others, resort to the rules of treaty interpretation of the Vienna Convention on the Law of Treaties ('VCLT') as well. The latter is an authoritative legal instrument that has codified the existing rules and techniques of treaty interpretation, put forward to aid judicial bodies[33] in resolving their doubts with regards to the exact meaning of the provision dealt with.

1. The Territorial Reference in Art. 2 (1) ICCPR

The ICCPR defines its territorial scope in Art. 2 (1) and obliges every State Party to ensure the rights recognized in the Covenant to all individuals within its territory and subject to its jurisdiction. This somewhat 'awkwardly formulated'[34] provision has been widely understood to mean that Covenant rights are to be guaranteed to all individuals within a state's territory and to all individuals subject to its jurisdiction.[35] The US is one of the few states that read this provision in a different manner.

a. The US Position

In the opinion of the US, persons who are not both within the respective territory *and* subject to the state's jurisdiction do not benefit from the treaty's protection.[36] In an attempt to substantiate its position and to present it as a long-established understanding and practice of the Covenant's applicability, the US argues using the *travaux préparatoires* and refers to its earlier statements before the HRC.[37] The US further relies

[31] Art. 2 (1) ICCPR stipulates that 'each 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…'; Art. 1 ECHR on its turn holds that 'the Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention'

[32] Cf. ICCPR art. 2 (1)

[33] Malcolm Shaw, *International Law* (Cambridge 2008) 932

[34] Cf. Manfred Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (Engel 2005) art 2, p 43, para 28

[35] See Nigel Rodley, 'Civil and Political Rights' in Catarina Krause and Martin Scheinin (eds), *International Protection of Human Rights: A Textbook* 110

[36] Cf. ibid 110; see also U.N. ESCOR Human Rights Committee, 'Summary Record of the 1405th Meeting: United States of America' (1995) U.N. Doc. CCPR/C/SR 1405, 7, 20. In its Second and Third periodic report, submitted in 2005, the United States government reiterated the view that 'the obligations assumed by a State Party to the International Covenant on Civil and Political Rights (Covenant) apply only within the territory of the State Party'. The United States stated this view again in the 2006 responses to the List of Issues to Be Taken Up in Connection With the Consideration of the Second and Third Periodic Reports of the United States of America and in its 2007 Observations Regarding the Human Rights Committee's General Comment 31

[37] Human Rights Committee, 'Consideration of reports submitted by States parties under article 40 of the Covenant' (2012) UN Doc. CCPR/C/USA/4, 142

on the ordinary meaning of the two conditions in Art. 2 (1) ICCPR connected by the conjunctive 'and'. This position, however, has been contested from the very moment of its articulation[38] and raises substantial problems. These shall be explored in the following sub-sections.

b. Rules of Treaty Interpretation in the VCLT

The Vienna Convention rules on treaty interpretation are considered declarations of pre-existing customary international law.[39] Arts. 31 to 33 VCLT covers the interpretation doctrines in international law. The first approach centers on the actual text of the provision in question, emphasizing the analysis of the words used.[40] The second approach considers the intention of the parties adopting the agreement, while the third approach looks at the object and purpose of the treaty as the most important tool in resolving ambiguities.[41] Thus, Art. 31 (1) VCLT requires in the first place a reading of the Covenant in good faith and consistent with the ordinary meaning of the terms used.[42]

Following this rule of interpretation, the US position seems to be the most natural one, considering the literal meaning of the 'and' as a conjunction between 'within its territory' and 'subject to its jurisdiction'.

However, what appears superficially to be the right answer leads to unsustainable results when considering some of the further norms in the ICCPR. The provision regarding the right to return to one's state[43] and the right not to be tried in absentia[44] presume exactly that individuals can be outside the territory of their state when exercising the rights in question. As Margulies[45] rightfully points out, these provisions would become a nullity if they would not protect persons at least temporarily outside a state's territory. Additionally, it would exclude from its reach individuals who are outside the state's jurisdiction but within its territory, such as foreign diplomats or members of foreign armed forces stationed on the territory pursuant to international agreements between the receiving and the sending state.[46] Thus, it makes more sense that Art. 2 (1) has to be read interpreted within the context of all of the substantive rights in Art. 6–27 ICCPR.[47] Otherwise, one would reach an interpretation that is inconsistent with the object and purpose of the treaty in the sense of Art. 31 (1) VCLT or to a result which, as Art. 32 (b) VCLT puts it, is manifestly absurd or unreasonable. It seems more logical to deem that Art. 2 (1) permits and requires a different construction.[48] This conclusion allows turning to the preparatory work and drafting history of the Covenant as a further means of interpretation, Art. 32 VCLT.

While the provision might have been drafted in a different manner that would have avoided the ambiguity, interestingly, the *travaux préparatoires* indicate that attempts to delete 'within its territory' and to replace 'or' for 'and' failed for different reasons.[49] One finds in the official records of the drafting process statements of the chief US delegate[50] that clearly show that including a reference to 'territory' in Art. 2 (1) ICCPR aimed at avoiding obligations to 'ensure' the rights of individuals in the territories occupied by the Allies after the Second World War. The obligation to *respect,* on the other hand, was not considered problematic. The US eschewed the responsibility to guarantee rights within the states with only recently recovered

[38] Milanovic (n 16)

[39] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro) Case* (2007) ICJ Rep ,160 ff.; *Indonesia/Malaysia Case* (2002) ICJ Rep, 625, 645-6; *Qatar v. Bahrain Case* (1994) ICJ Reports, 6, 21–2

[40] Shaw (n 34) 933

[41] Shaw (n 34) 932

[42] Vienna Convention on the Law of Treaties (adopted 23 May, 1969, entered into force 27 January 1980) 1155 UNTS 331, 8 ILM 679, art 31 (1)

[43] Cf. the wording in Art. 12 (4) ICCPR

[44] Art. 14 (3) d ICCPR provides for 'the right to be tried in his presence' and outlaws *in absentia* criminal trials.

[45] Peter Margulies, 'The NSA in Global Perspective: Surveillance, Human Rights and International Counterterrorism' (2014) 82 Fordham Law Review, 2143

[46] Michal Gondek, *The Reach of Human Rights in a Globalising World: Extraterritorial Application of Human Rights Treaties* (Intersentia, 2009) 132

[47] Dominic McGoldrick, 'Extraterritorial Application of the International Covenant on Civil and Political Rights' in Fons Coomans and Menno T. Kamminga (eds), *Extraterritorial Application of Human Rights Treaties* (Oxford 2004) 45

[48] Thomas Buergenthal, 'To Respect and to Ensure: State Obligations and Permissible Derogations' in Louis Henkin (ed), *The International Bill of Rights* (Columbia University Press 1981) 74

[49] Annotations on the Text of the Draft International Covenants on Human Rights, GAOR 10th SessionAnnexes, UN Doc. A/2929 (1955) para II, chapter 5, para 4; Report of the Third Committee, UN GAOR, 18th Session Annexes, UN Doc. A/5655 (1963) para 18

[50] See U.N. Human Rights Committee (Sixth Session) 'Summary Record of the Hundred and Ninety-Third Meeting' (1950) UN Doc. E/CN.4/SR. 193, 13

democratic institutions.[51] Potential inconsistencies with the international law of occupation had to be considered as well.[52]

The facts illustrated above show a very different position by the US Government and a diverse meaning of the terms. Thus, the reading of the US cannot be considered a long-established practice.

In addition it should be also noted that the International Court of Justice has endorsed the extraterritorial applicability of human rights obligations in its 'Wall' Advisory Opinion.[53]

c. Why the Narrow View is not Persuasive in the Surveillance Context

Although the stance of the US was reviewed and conceived as inconsistent with effective international law in general, in order to strengthen this finding it is important to see how the US position would perform in the surveillance context.

As the HRC has stressed in its General Comment ('GC') on the nature of legal obligations imposed by the Covenant,[54] every State party has a legal interest in the performance by every other State party of its obligations. Bearing this in mind, the US reading of the territorial scope of the ICCPR brings a couple of interesting consequences along.

The first one is that it allows states to perform illegal or arbitrary surveillance on anyone outside of their own territory or outside of their jurisdiction.[55] This automatically means that the Covenant secures the privacy of i.e. Americans only against arbitrary and illegal interferences by their own state, but would leave them unprotected against intrusions by every other state agency in the world.[56] However, this result most certainly conflicts with the very nature of human rights, to which every human being is entitled by the simple fact of being human and a bearer of human dignity.[57] Human Rights cannot be assimilated to social compacts, nor depend for their applicability on 'morally arbitrary criteria' such as the mere accident of birth.[58] In the words of Ronald Dworkin, '[t]he domain of human rights has no place for passports'.[59]

The second consequence to consider is that with this reading, the task of each state to protect its own subjects from the spying activities conducted by all other states would be impossible to accomplish. This is true to the extent that privacy intrusions would become something ordinary, potentially defeating the object and purpose of the treaty with regards to the right to privacy. Such an understanding of Art. 2 (1) ICCPR would not only offer very little protection with regards to privacy, but most the protection offered for most of the other ICCPR rights would be undermined. And here is where the line must be drawn – where even a small part of the Covenant's guarantees cannot be fulfilled in any reasonable way as a result of a particular understanding of the treaty, then this understanding is most certainly inadequate.[60]

The illustrated points make it clear that the advocated understanding of the Covenant's territorial scope by the US is unsustainable under international law. The reference to a state's territory in Art. 2 (1) ICCPR is not to be read as excluding extraterritorial application *per se*.

Now that this has been established, the rather similar jurisdictional clauses of the two provisions can be further examined.

2. State Jurisdiction under Art. 1 ECHR and Art. 2 (1) ICCPR

The next challenge is to establish what exactly being under a state's jurisdiction means and entails. In order to elaborate the concept, which would be applicable to foreign surveillance activities, the following section outlines the major findings of the HRC and the ECtHR on extraterritoriality. Both bodies have had the opportunity to decide on whether the human rights treaties in question apply outside of a State's party territory.

---

[51] Margulies (n 43) 2143

[52] ibid

[53] Cf. *Advisory Opinion to the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) ICJ Rep 2004, 136 para. 106–113

[54] U.N. Human Rights Committee (2187th meeting), 'General Comment No. 31 (80), Nature of the General Legal Obligation on State Parties to the Covenant (29 March 2004) UN Doc. CCPR/C/21/Rev.1/Add. 13, para. 2

[55] Cf. Alex Sinha, 'NSA Surveillance Since 911 and the Human Right to Privacy' (2013) 59 Loy. L. Review, 902

[56] ibid

[57] Cf. Heiner Bielefeld, 'Philosophical and Historical Foundation of Human Rights' in Catarina Krause and Martin Scheinin (eds), *International Protection of Human Rights: A Textbook* (Sastamala 2012) 5

[58] Cf. Sinha, (n 57) 902

[59] Ronald Dworkin, *Is Democracy Possible Here?: Principles for a New Political Debate* (Princeton University Press 2008), 48

[60] Cf. Sinha (n 57) 902

a. First Extraterritorial Steps

For the simple reason that 'jurisdiction' has emerged as the basis of sovereignty and state's sovereign powers, the original notion of jurisdiction is necessarily linked with the idea of territorial powers.[61] That is why jurisdiction is closely related to the national territory.[62] However in the interventionist age[63] we live, with the growth of operations conducted abroad and the ever-increasing number of individuals brought under some form of foreign *de facto* control, the question of human rights treaties' applicability although vague in terms of the exact guarantees' scope is quite significant. Taking this in account, the ECtHR has only accepted in exceptional cases that acts carried out by the Member States outside their territories can be an exercise of jurisdiction in the sense of Art. 1 ECHR.[64]

The territorial scope of the ECHR has been a point of contention for quite some time. Although Art. 1 ECHR has received some fair attention in the Court's case law; the ECtHR's position is far from uniform. It had a promising start with the *Loizidou* case,[65] where the Court accepted that the treaty has a certain degree of extraterritorial effect, coupling the Convention's application with the requirement of effective control employed by a State Party in a certain area. What mattered was the question of effective control, regardless of whether it was based on an unlawful act, i.e. violation of the territorial state's sovereignty.[66] In the later judgement of *Cyprus v Turkey*, the justices of the Grand Chamber reaffirmed their position, adding to the previous argumentation the need to reject the otherwise resulting 'regrettable vacuum in the system of human-rights protection'.[67]

In a similar cautious manner, the early HRC only ruled in favour of extraterritorial application in 'exceptional circumstances', such as when states acted against their own citizens living abroad.[68] However, it must be also acknowledged that in comparison to the ECtHR, the Committee's degree of practice in the matter of extraterritoriality is more limited by the simple fact that it receives fewer complaints than its European counterpart. As will be illustrated below, the consequence is that the Committee often turns to the judgements delivered by the ECtHR for interpretation help.

In the so called *Passport cases*,[69] the HRC found that States parties are responsible for infringements of the Covenant committed by their foreign diplomatic representatives. Further, considering the cases of individuals kidnapped by Uruguayan agents in neighbouring countries, the Committee held that States parties are liable for the actions of their agents on foreign territory.[70] The HRC thus accepted the extraterritorial application of the ICCPR in cases where state agents exercised authority and control over individuals, rather than over areas. This same approach used by the ECtHR in one of its early *Cyprus cases*,[71] where it had found that States parties are 'bound to secure the rights and freedoms to all persons under their actual authority'. In other words, what mattered was the relationship between the individual and the state and not where the alleged violation occurred.[72]

b. Jurisdictional Approaches after Bankovic

What looked like an auspicious (although not entirely uniform) beginning that kept pace with recent developments in the international community, took a step back with the *Bankovic* admissibility decision.[73] In this case, the ECtHR found that the victims of an air strike on a TV station in Belgrade had never been 'within

---

[61] European Commission of Human Rights, 'Commission Report' (12 October 1989) Series A no. 99, p. 24 § 167

[62] Rick Lawson, 'Life after Bankovic: On the Extraterritorial Application of the European Convention on Human Rights' in Fons Coomans and Menno Kamminga (eds), *Extraterritorial Application of Human Rights Treaties* (Intersentia 2004), 87

[63] ibid. 84

[64] Cf. Pablo Antonio Fernández-Sánchez, 'The Scope of Obligations under the European Convention of Human Rights' in Javier García Roca and Pablo Santolaya (eds) *Europe of Right: A Compendium on the European Convention of Human Rights* (Martinus Nijhoff Publishers 2012) 36

[65] *Loizidou v. Turkey* App no 15318/89 (ECtHR (GC), 23 March 1995)

[66] Cf. Milanovic (n 16) 39

[67] *Cyprus v. Turkey* App no. 25781/94 (ECtHR (GC), 10 May 2001) para 78

[68] Michael Dennis, 'Application of Human Rights Treaties Extraterritorially During Times of Armed Conflict and Military Occupation' (2005) American Journal of International Law 88–89

[69] No. 31/1987; No. 57/1979; No. 77/1980; Nos. 106, 108/1981; No. 125/1982

[70] UNHRC 'Lopez Burgos v Uruguay, Communication No. 52/1979' (29 July 1981) UN Doc CCPR/C/13/D/52/1979 § 12.3; IACHR 'Lilian Celiberti de Casariego v Uruguay, Communication No. 56/1979 (17 July 1979) UN Doc CCPR/C/OP/1 § 10.3

[71] *Cyprus v. Turkey* App no 6780/74 and 6950/75 (ECtHR, 26 May 1975) 136 para 8

[72] Cf. Martin Scheinin 'Extraterritorial Effect of the International Covenant on Civil and Political Rights' in Fons Coomans and Menno Kamminga (eds) Extraterritorial Application of Human Rights Treaties (Intersentia 2004) 73

[73] Schiedermair (n 17)

the jurisdiction' of the NATO Member States. The Court observed that only effective control – an exercise of all or some public power – over a territory and its inhabitants due to a military occupation or an explicit agreement could bring the situation within the jurisdiction of the 'occupying' state. The mere repercussions of States parties' actions, i.e. dropping bombs over Belgrade, would not trigger control over the territory or individuals in question.[74] This approach, clearly leaning towards the pronouncement of the Convention's extraterritorial application as an exception, has casted quite some doubt on the Court's reasoning, which has been a point of critique and discussion ever since.

The decision in the *Issa* case[75] led to further confusion with its observation that 'Art. 1 of the Convention cannot be interpreted so as to allow a State party to perpetrate violations of the Convention on the territory of another State, which it could not perpetrate on its own territory'. The Court stipulated that even short-term military operations in a territory brought the individuals there under the jurisdiction of the acting state. In the *Ilascu* case,[76] the Court affirmed the triggering effect of military control in an area, but this time it reduced the requirement to 'overall control'.

This so-called 'more generous approach'[77] was later followed in the *Al-Skeini*[78] judgement as well, where the Court explained that the test of jurisdiction could be met either through control over an individual or over a certain area. In addition, a state can exercise effective control either directly, through its own armed forces, or by means of a 'subordinate local administration'.[79] Thus, it would seem that the ECtHR was moving away from the view that jurisdiction is an all-or-nothing matter,[80] trying to correct to some extent the *Bankovic* findings by reducing the degree of control required over a territory. A further development in the Court's approach was brought by the case of *Öcalan v Turkey*,[81] a case involving the handing-over of a suspect of terrorist-related crimes to Turkish officials in Kenya. The ECtHR noted that the suspect was 'effectively under Turkish authority and therefore within the jurisdiction of Turkey' after the handing-over was completed.[82] Simplifying this statement means that the State party in question does not need to exercise all public powers, for even some exercise of public powers is sufficient to trigger jurisdiction, although not in an exclusive manner with regard to all other states and their rights.

In the meantime, the HRC, which from its very inception has sought a way to provide a reading of Art. 2 (1) ICCPR that renders appropriate legal protection and had therefore followed the disjunctive interpretation, extended the application of the Covenant to actions of state authorities in occupied territories as well.[83] For example, as the Committee has stated in its recent comments on Israel, the latter bears responsibility for implementation of the ICCPR within Israel, as well as the Occupied Palestinian Territories in the West Bank and Gaza[84] where Israel exercised effective jurisdiction and effective control. The HRC's line of arguments appears to follow *Bankovic*, that is, it is based on an 'effective control' approach.[85] The Committee has applied this approach in a number of different contexts where the state acts or takes measures on the territory of another state and these have an effect on persons within that other state's territory.[86] In GC 31 the Committee reaffirmed its position, asserting that a State Party must provide for the Covenant's rights to anyone within its power or effective control, even if not situated within its respective national borders and without concern for the circumstances in which such power or effective control was obtained.[87] In other words, in the view of the Committee, states are always bound to both respect and ensure that individuals

---

[74] ibid

[75] *Issa v Turkey* App no 31821/96 (ECtHR 16 November 2004) para 71; confirmed in *Isaak et al. v Turkey* App no 44587/98 (ECtHR 28 September 2006); *Pad et al. v Turkey* App no 60167/00 (ECtHR 28 June 2007); and *Andreou v Turkey* App no 45653/99 (ECtHR 3 June 2008)

[76] *Ilascu et al. v MD a. RUS* App no 48787/99 (ECtHR (GC), 8 July 2004, 2004) VII 310 316

[77] Rick Lawson 'The European Convention on Human Rights' in Catarina Krause and Martin Scheinin (eds) *International Protection of Human Rights: A Textbook* (Abo Akademi University 2009) p 428

[78] *Al-Skeini et al v the UK* App no 55721/07 (ECtHR (GC), 7 July 2011) para 130f

[79] *ibid*, para 138

[80] Margulies (n 43) 2147

[81] *Öcalan v. Turkey* (2003) 37 EHRR 238

[82] ibid 98

[83] Sarah Joseph, Jenny Schultz and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (OUP 2004) p 88

[84] (2003) UN doc CCPR/CO/78/ISR; see also Concluding Observations on Israel, (1999) UN doc CCPR/C/79/Add. 93, para 10. However, where powers had been effectively transferred to the Palestinian Council, Israel could not be held responsible

[85] Dominic McGoldrick 'Extraterritorial Application of the International Covenant on Civil and Political Rights' in Fons Coomans and Menno Kamminga (eds), *Extraterritorial Application of Human Rights Treaties* (Intersentia, 2004) 65

[86] ibid 55

[87] 'General Comment 31' [80], (2004) CCPR/C/21/Rev.1/Add. 13, 10

receive maximum protection of their human rights.[88] Through this position the HRC has officially developed a case law that some scholars have criticized for being purposive[89] and rather goal-oriented. While this presumption may or may not be true and could be the topic of an entirely different investigation, it demonstrates one of the core problems of extraterritoriality – namely that human rights protections are necessarily extraterritorial. This issue will be addressed in a moment under 2. d).

c. The Test of 'Subject to its Effective Control' in the Surveillance Context

As it was illustrated above, the effective control over territory or over individuals test represents the best synthesis of the ECtHR's current extraterritorial jurisprudence, supported by the HRC as well. However, this approach was put into place long before one could even consider the issue of foreign surveillance and its impact on the discussion.

The 'effective control' notion is adequate to analyse the actions in real time taken abroad by state agents,[90] but in the cyber domain, the physical control over persons or territory is not very useful.[91] The NSA has the capacity to remotely control and filter much of the communications of a foreign national abroad and, as indicated in the press, the agency can break different forms of encryptions thanks to so-called 'back-doors' it has engineered in many software systems.[92] In addition, the implantation of tiny radio transmitters in most of the computers produced in the US grants the NSA the capacity to gain control over computers not connected to the Internet.[93] Considering also that much of the Internet traffic is routed through the US, makes the picture complete – physical control does not play a role at all. That is why in order to answer the question how surveilling a foreign national's communications renders that person subject to the surveilling state's jurisdiction,[94] the concept needs to be adapted to the cyber context. A narrow standard does not do justice to the rapidly evolving technology, but an official solution has not been established yet, although one of the first cases concerning external communications' interception is already being dealt with in Strasbourg.[95]

In this regard, Margulies suggests the virtual control test as an approach that at least for now can meet this challenge.[96] Applying this standard has two advantages: first, it works closely with the notion of control developed and required in the jurisprudence discussed above; second, it considers and bridges the changing technological circumstances that any practitioner would face when dealing with questions of jurisdiction triggering human rights obligations in surveillance cases. The intelligence agencies under scrutiny are perfectly capable of controlling lives and private information with the press of a button. Without a proper assimilation of the effective control test in cyberspace these intrusions would remain unaddressed and would run counter to substantial human rights principles. Privacy rights should be protected even when interferences have been initiated in a place different than the affected individuals' abode. The virtual control test is thus preferable when assessing the extraterritorial application of privacy interests in cases of foreign surveillance.

d. Type of State Obligations in the Extraterritorial Application

What has become clear from the above sub-sections is that both the ECtHR and the HRC, certainly not uninfluenced from each other's findings and interpretations, apply the treaties in question outside of the national borders of the States parties. The current stance of both bodies is to answer in affirmative the question of jurisdiction where some kind of public power has a controlling effect over an area or an individual abroad. What needs a point of clarification, however, is what exactly states are obliged to do when their jurisdiction is triggered.

---

88 Margulies (n 43) 2145
89 ibid 2144
90 ibid 2148
91 David Clark and Susan Landau, 'Untangling Attribution' (2011) Harvard NSJ 533
92 See Scott Shane, 'Nor Morsel Too Miniscule for All-Consuming N.S.A.' *The New York Times*, (New York City, 3 November 2013) <http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html? pagewanted=all&_r=0>
93 See David E. Sanger and Thom Shanker, 'N.S.A. Devises Radio Pathway into Computers' *The New York Times*, (New York City, 15 January 2014) < http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected -to-internet.html>
94 Cf. Ashley Deeks, 'Does the ICCPR Establish an Extraterritorial Right to Privacy?' (*Lawfare Blog*, 14 November 2013) <http://www.lawfareblog.com/2013/11/does-the-iccpr-establish-an-extraterritorial-right-to-privacy/#.Ut26AaMo6po>
95 *Big Brother Watch and Others v. UK* (App no 58170/13 (ECtHR, lodged on 4 September 2013)
96 Margulies (n 43) 2149

In this regard it is important to turn again to the original treaty provisions. While the ICCPR text requires states to 'respect and ensure'[97] the rights in the Covenant and, as it was illustrated above, the Committee has gladly taken up this wording in its demands for effective rights protection, Art. 1 ECHR speaks of 'securing' the respective rights and freedoms. However, despite the differences in the wording of these treaty provisions, it has become customary to apply the tripartite typology of respect – protect – fulfil when assessing state's obligations under a human right treaty.[98] One can also categorize the duty to respect as closely corresponding to negative obligations,[99]s and the other two dimensions (protect and fulfil) to positive obligations.[100] Since 'to secure' in Art. 1 ECHR and 'to respect and to ensure' in Art. 2 (1) ICCPR encompass both negative and positive obligations, it can be acted on the assumption that both treaties mean the same.

Now, the problem with the extraterritorial application is constituted by the fact that interventions abroad take place in forms other than extensive and long-term military operations and occupations. In many cases, there are actions that can and are accomplished in a matter of days or even hours. Under these circumstances, the foreign state acting abroad cannot be expected to also positively ensure or protect human rights, for it does not have the respective powers to adopt any legislative, judicial or administrative or other appropriate measures in order to fulfil its positive legal obligations. It can only make sure to respect and not to interfere with the rights of the individuals. A further difficulty arises out of the fact that the bodies entrusted with the application and interpretation of the provisions have either left the question of the exact nature of the obligation unaddressed or have opted for an 'all-or nothing' approach. In other words, the approach is everything but conclusive.

Some voices in the literature suggest a completely different solution and advocate a *relational* or *contextual* assessment in light of the particular right in the respective situation.[101] It seems, however, like a rather pedestrian method to leave the determination of extraterritoriality and the state obligations it triggers to the interpretation of what constitutes a human right and what constitutes a human right violation.[102] Bearing this in mind, the present contribution follows the positions of Milanovic[103] and Margulies,[104] who make a plausible argument suggesting that the duty to ensure a right should be limited to the cases where the individual is both within a state's territory and subject to its jurisdiction. Since states always remain in full control of their organs and agents,[105] they are also perfectly capable of complying with their negative obligations. The 'moral logic of universality'[106] is thus also brought into balance, while jurisdiction still serves as a limiting factor for the normally far more tedious positive obligations.

Now that the type of state obligations in the extraterritorial application of human rights has been established and the test of 'effective control' has been adapted to the cyber context, the discourse can be further brought to the actual privacy provisions and their details in the ECHR and the ICCPR.

B. Substance of the Right to Privacy

In order to make an authoritative assessment of the human rights situation in the context of foreign surveillance, it is first necessary to establish what exactly the HR to privacy entails and what individual interests fall under it. The areas presently covered, however, are those most relevant to the NSA surveillance program. Correspondingly, in the following section the terms of 'privacy' and 'correspondence' as presented in Art. 17 ICCPR and Art. 8 ECHR will be dealt with.

---

[97] Cf. art 2 (1) ICCPR

[98] Martin Scheinin, 'Characteristics of Human Rights Norms' in Catarina Krause and Martin Scheinin (eds) *International Protection of Human Rights: A Textbook* (Abo Akademi University, 2009) 27

[99] The ECtHR has affirmed that the obligation to 'secure' does not only refer to the retention of offending or violating acts by the state authorities, but that the obligation under Art. 1 ECHR is broader than that. The Court has also come to accept that domestic authorities should also protect individuals against private assassins or domestic violence, see *Osman v. UK* App no 23452/94 (ECtHR (GC), 28 October 1998) Reports of Judgements and Decisions 1998-VIII, esp. paras. 115–116

[100] Scheinin (n 100) 28

[101] Scheinin (n 74) 73, according to which the issue of jurisdiction cannot be isolated but is inherently linked with issues such as compatibility *ratione personae* and even to substantive issues such as whether there was a violation of a human right

[102] Cf. Scheinin's suggested formula (n 74) 79

[103] Milanovic (n 16) 46–48

[104] Margulies (n 47) 2149

[105] Beth Van Schaack, 'The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change' (2014) 90 International Law Studies 49–52

[106] Milanovic (n 16) 47

1. The 'Right to Privacy' in Art. 17 ICCPR and the 'Right to Private Life' in Art. 8 ECHR – Two Codifications, One Legal Meaning

It should be noted first that the two provisions differ in their literal composition. Art. 8 ECHR uses the term 'private life', Art. 17 ICCPR speaks of 'privacy'. The following section shall examine to what extend the provisions in question cover the same individual interests.

The broadness of the term 'private life' and its definition have caused some interpretation difficulties in academia.[107] Up until now, the Strasbourg Court has not deemed it necessary to present an exhaustive definition of the notion of 'private life',[108] transforming Art. 8 ECHR into a 'general charter of individual autonomy'.[109] This has allowed the Court to take a flexible approach in the assessment of the facts in every individual case.[110] Following, however, the Court's (and earlier the Commission's) case-law one can narrow down certain criteria that help in determining the protected interests.

At the heart of the concept is the notion of private space into which no-one is entitled to enter, raising an aspect of the right to be left alone free from unwelcome interferences[111] and to conduct one's life 'in a manner of one's own choosing'.[112] Besides the guarantee of private space, the provision comprises protection of one's personal information. Both the Commission and the Court have affirmed that collection and storage of personal data concern 'private life' and fall within the scope of protection granted by Art. 8 (1) ECHR.[113] Thus, collection of information by officials without the individual's consent will interfere with his right to respect for his private life.[114] The same applies for electronic surveillance activities, telephone tapping and email interception - these infringe upon the private life of the individual as well.[115] Emphasising that the scope of private life goes beyond the notion of privacy in the meaning of secrecy, the ECtHR has established that 'private' is not to be read as referring to the question of disclosure or nondisclosure but to 'the right to choose certain intimate aspects of one's life, free of government intrusion'.[116]

Interestingly, one encounters the same questions of interpretation with regard to the term 'privacy' in Art. 17 ICCPR. Its meaning has not been authoritatively clarified in the General Comments of the Human Rights Committee or its corresponding case-law.[117] Privacy, however, has been widely understood as 'the right to be left alone'[118] and narrowly as a right to control information about one's self.[119] A useful definition can be found in *Joseph, Schultz and Castan,*[120] which stipulates that privacy encompasses 'freedom from unwarranted and unreasonable intrusion into activities […] belonging to the realm of individual autonomy'.[121] 'Individual autonomy' on its turn refers to 'the field of action that does not touch upon the liberty of other', where one may withdraw from the eyes of the public to 'shape one's life according to one's own wishes and expectations'[122] and to strive for self-realization. Individual autonomy also covers action with others and thus entails a claim to private communication with the respective others. Privacy under Art. 17 ICCPR also holds guarantees for a right of intimacy, i.e. secrecy from the public of private characteristics, actions or personal data,[123] which is of a particular importance for the present study.

The listing of the most commonly encountered components of the 'right to privacy' and of 'the right to private life' show that despite the linguistic differences in the two English texts, 'privacy' within Art. 17 ICCPR and 'private life' under Art. 8 ECHR mean the same thing.[124] The fact that practitioners and scholars

---

[107] Christoph Grabenwarter, *The European Convention on Human Rights: Commentary* (Beck/Hart 2014) para 189
[108] Cf. *Niemietz v Germany* App No 13710/88 (ECtHR (Chamber),16 December 1992) 16 E.H.R.R. 97
[109] Cf. Mark W. Janis, Richard S. Kay and Anthony W. Bradley, *European Human Rights Law: Text and Materials* (3rd edn, OUP, 2008) 374
[110] David Harris, Michael O'Boyle, Ed Bates and others, *Law of the European Convention on Human Rights* (OUP 2009) 36
[111] ibid 367
[112] *Pretty v United Kingdom* (Application No. 2346/02), ECHR (Fourth Section), Judgement of 29 April 2002, 35 EHRR 1
[113] Jochen Frowein und Wolfgang Peukert, Europäische Menschenrechtskonvention, Art. 8, p. 290
[114] Harris, O'Boyle, Bates and others (n 112) 368
[115] ibid 367
[116] Cf. Janis, Kay and Bradley (n 111) 426
[117] Cf. Joseph, Schultz and Castan (n 85) 477
[118] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1980) 4 Harvard Law Review 193, 195
[119] Alan F. Westin, *Privacy and Freedom* (Athenaeum 1967) 7; Charles Fried, 'Privacy' (1968) 77 Yale Law Journal 483
[120] Joseph, Schultz and Castan (n 85) 467
[121] Elisabeth Wilborn, 'Revisiting the Public/ Private Distinction: Employee Monitoring in the Workplace' (1998) 32 Georgia Law Review 833
[122] Nowak (n 35) 288; Fernando Volio, 'Legal Personality, Privacy and the Family' in Louis Henkin (ed), *The International Bill of Rights* (Columbia University Press 1981) 193–5
[123] Nowak (n 35) 387, para 21
[124] Cf. Nowak (n 35) 385 para 16

dealing with the normative substance of Art. 17 ICCPR often resort to the findings of the Strasbourg Court for interpretation helps to affirm the proximity of the two provisions.

2. Correspondence

For the sake of completeness, the highly relevant term 'correspondence' will be carefully examined.

Art. 8 (1) ECHR includes an explicit reference to the right to respect for one's correspondence as an autonomous interest, which is often understood as the right to uninterrupted and uncensored communications with others.[125] Interferences with this right however often affect and overlap with private life interests, which has led in the praxis to their collective consideration. The ECtHR has based its wiretap judgements partly on the protection of private life and partly on the right to correspondence, keeping pace with developments in technology and ascertaining that telephone communication is a form of correspondence.[126] To that effect every means of communication controlled, supervised and/or protected domestically by the state like postal correspondence is to be qualified as a correspondence in the sense of Art. 8 (1) ECHR.[127] The nature of the operating agency itself is considered irrelevant.[128]

Similar to the structure of Art. 8 ECHR, Art. 17 ICCPR also protects individual correspondence as a separate interest. Here, correspondence is also understood to encompass not only written letters, but all forms of distance communication, i.e. by telephone, fax, email, etc. The emphasis of the corresponding protection lies in the secrecy of the communication. Therefore, interceptions, inspections and other forms of secret surveillance would necessarily affect the very core of this interest.

As Sinha rightfully points out, reports on the NSA program have thus far exposed three substantial ways in which the US government is possibly infringing the right to privacy under the ICCPR These are: 1) Through the gathering or examination of emails; 2) Through the recording or interpretation of phone calls; and 3) By accumulating or reviewing transactional data. The first two fall within the protection framework of correspondence, while the third refers to privacy more generally.[129]

C. Interference with Privacy Interests

Both Art. 17 (1) ICCPR and Art. 8 (1) ECHR give a good summary of the interests they protect and which, when interfered with, might lead to violation of the respective provisions. However, what exactly is regarded as an interference is a different and curious matter, which will be clarified in the following lines.

In their early decisions on secret surveillance activities, the judges of the ECtHR defined the kind of state interference that deserves the Court's attention.[130] Laying down a milestone for future references, the Court established that Art. 8 ECHR is only able to deploy its full protection capacity if the mere existence of legislation or secret measures is considered an interference. The Court has opted for this approach bearing in mind that 'the mere existence of the legislation' generated a 'menace of surveillance' which necessarily affects the liberty of interaction between users of communication services and hence presents an 'interference' by a public authority with the right to respect for private life and correspondence.[131] The Strasbourg judges continued this line of thoughts in the case of *Malone v the UK,*[132] where they reaffirmed their position by holding that the existence of legislation that allowed the interception of phone calls amounted to infringement on the applicant's rights. In *Liberty and others v the UK* the Court extended its position to general programs of surveillance as well as targeted wiretapping of private conversations.[133]

As to Art. 17 (1) ICCPR, clarification on what constitutes an 'interference' with privacy rights is also required. However, the line of arguments regarding the decisive interference with the interests protected by the provision is not as firmly established as in the case of Art. 8 (1) ECHR. A difficulty arises also by the fact that the rather outdated General Comment 16 on privacy does not provide any conclusive guidance on

---

[125] Cf. Harris, O'Boyle, Bates and others (n 112) 380

[126] *Klass and others v Germany* App no 5029/71 (ECHR (Plenary), 6 September 1978) 2 E.H.R.R. 214

[127] Frowein and Peukert, (n 115) 314 para 48

[128] ibid

[129] Sinha (n 57) 917

[130] The primary cases cited in ECtHR jurisprudence are *Klass and others v Germany* Appl no 5029/71 (ECtHR (Plenary), 6 September 1978); *Malone v United Kingdom* App no 8691/79 (ECtHR (Plenary), 2 August 1984); *Weber and Saravia v Germany* App no 54934/00 (ECtHR (Third Section), 29 June 2006); *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* App no 62540/00 (ECtHR (Fifth Section), 28 June 2007); *Liberty and Others v United Kingdom* App no 58243/00 (ECtHR (Fourth Section), 1 July 2008); and *Iordachi and Others v Moldova* App no 25198/02 (ECtHR (Fourth Section), 14 September 2009)

[131] *Klass and others v Germany* (n 133) para 41

[132] *Malone v United Kingdom* (n 133)

[133] Cf. *Liberty and others v the U*nited Kingdom (n 133) para 63

what represents an interference within the meaning of Art. 17 ICCPR. Yet international human rights bodies, including the Committee,[134] have opted once again to follow the lead of their European counterpart and have made it clear that surveillance regulations or practices may interfere with privacy, and that the mere collection and storage of data—even data that is publicly accessible—may be an 'interference' that falls within the constraints of Article 17.[135] The voices in the academic literature seem to advocate a similar approach.[136] *Volio* suggests an even broader reading of Art. 17, which should protect from interferences with any means of receiving and keeping ideas or information in private.[137]

Presently, the ECtHR's argument plays an essential role[138] in Europe and across the Atlantic. It means that a violation of privacy rights is supposable even when an individual does not experience a noticeable harm.[139] This discovery is of importance not only in 'regular' surveillance cases, but also where collective data processing is at stake and where it is often nearly impossible for individuals to demonstrate that their personal data was collected or processed.[140] The psychological effect of the uncertainty in those circumstances is sufficient to interfere with the freedom to engage in private behaviour.[141]

Bearing this expansive view[142] in mind, determining what constitutes an interference with privacy is a rather rewarding task and would include collection of metadata,[143] every form of telecommunication, including over the Internet,[144] GPS tracking[145] and audio-visual observations.[146] In fact, this approach allows for the consideration of the entire range of foreign surveillance activities conducted by the NSA, GCHQ and their allies' agencies. Interference with Art. 8 ECHR and Art. 17 ICCPR is thus at hand.

D. Legality of the Interference

Ascertaining that foreign surveillance activities as conducted in the present case interfere with the interests protected by the discussed provisions is not the challenging part in the present contribution. What needs to be addressed is whether intrusions with the privacy 'privilege'[147] of the individual can be justified under Art. 17 ICCPR and Art. 8 ECHR.

Art. 8 (2) ECHR provides a list of the reasons a government may use to justify an interference with the right to privacy. This provision permits a public authority to interfere so long as its actions are 'in accordance with the law', 'necessary in a democratic society' and pursue 'legitimate aims'. The 'legitimate aims' include among others also crime and disorder prevention and protection of the rights of others. Art. 17 ICCPR does not include an explicit constraint clause allowing for restrictions in the interest of public order or similar ends, providing instead that 'no one should be subjected to arbitrary or unlawful interference'. The conjunction 'arbitrary or unlawful' reveals that not only unlawful but also arbitrary attacks on privacy are prohibited.[148]

Both norms and their limitations are rather broadly formulated and have undergone considerable interpretations by the HRC and the ECtHR. In the years of practice the two bodies have aligned their approaches and have established very similar assessment criteria. These examine in the first place whether the interference in question is lawful/in accordance with the law. As a next step they look for the intrusion's legitimate aim. Lastly, if a legitimate aim is given, the criterion of proportionality must be satisfied. It should be noted that in the following, only cases and provisions relevant to foreign surveillance activities shall be considered.

---

134 Cf. J.*R.T. and W.G. Party v Canada*, no 104/1981, § 8 (c)

135 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 on Civil and Political Rights' (2014) <https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf>

136 Cf. Nowak (n 35) 401–402

137 Volio (n 124) 198

138 Cf. Paul De Hert and Franziska Boehm, 'The Rights of Notification after Surveillance is over: Ready for Recognition?' in *Digital Enlightment Yearbook 2012* Jacques Bus, Malcolm Crompton, Mireille Hildebrandt, George Metakides (eds) (IOS Press 2012) 24

139 See Milanovic (n 16) 67

140 ibid

141 *Dudgeon v United Kingdom* App no 7525/76 (ECtHR, 22 October 1981) 40–41

142 Milanovic, (n 16) 66.

143 *Malone v the United Kingdom* (n 133) 84

144 Cf. *Liberty and Others v United Kingdom (n 133)* 56; *Kennedy v United Kingdom* App no 26839/05 (ECtHR, 18 May 2010) 118

145 *Uzun v Germany* App no 35623/05 (ECtHR, 2 September 2010) 49–53

146 *El Haski c Belgique* App no 649/08 (ECtHR, 25 September 2012) 102

147 Cf. Volio (n 124) 195

148 Nowak (n 35) 381 para 9

1. Prescribed by Law

In order to fulfil this criterion, both Art. 8 (2) ECHR and Art. 17 ICCPR require an authorization under national law to interfere with privacy interests. Such entitlement must be based on generally accessible provisions of law proclaimed prior to interference.[149] The HRC has made this clear by indicating that the interference can be justifiable only in the cases actually envisaged by law.[150] On the European scene, where owing to the considerable case law on the matter the criterion's fundament is quite solidly established, this approach was first articulated in the case of *Klaas and Others v Germany*,[151] one of the first surveillance cases of the ECtHR. Although the Court did not find a violation of the applicant's right to privacy, it identified the applicable test to determine whether and when secret surveillance activities infringe on a person's basic human rights.[152] Accordingly, the law that allows the intrusion has to be clear enough so that concerned individuals can inform themselves about the applicable terms.[153]

In *Malone*,[154] where the government of the UK did not operate under a single comprehensive set of rules, but under common law doctrines, the Court asserted that it was not clear what legal standards applied[155] to regulate the government's activities. On the basis of the case, it further developed the requirements of accessibility, foreseeability and compatibility with the rule of law and has affirmed them in the subsequent surveillance cases. A breach of these requirements on the domestic level automatically leads to violations of international human rights provisions.[156] The HRC equally supports this position.[157]

When taking a closer look, one discovers in the case-law of the Strasbourg Court and in the communications decided before the HRC that not all accessibility and foreseeability elements have to be specified in primary legislation. However, secondary sources could satisfy this requirement 'only to the admittedly limited extent to which those concerned were made sufficiently aware of their contents'.[158] Although both the ECtHR and the HRC often approach the two requirements as a conjoined matter, an attempt to differentiate their particular demands shall be made in the following section.

a. Accessibility

The criterion of accessibility aims at transparency[159] and mandates that exceptions to Art. 17 ICCPR or Art. 8 (1) ECHR cannot be secret.[160] Individuals must be given the opportunity to familiarize themselves with the relevant rules. Against security concerns that more detailed public information about surveillance activities would jeopardize the efficiency of such operations,[161] the Strasbourg Court applies as a reference the case of *Weber* where the German government had incorporated guidelines and limitations in the primary legislation itself.[162] The accessibility of the information had clearly not had any adverse effect on the surveillance activities, 'strategic monitoring' or the subsequent uses and sharing of the gathered telecommunications information with other security agencies. It should also be noted that the Court's approach does not imply full data disclosure or exposure of internal regulations applicable in the respective surveillance agencies. It simply establishes a certain level of accessibility that should be maintained.[163]

The authority for the PRISM program appears to derive from the FISA Amendments Act of 2008 ('FAA'), which includes a regulation for the premeditated targeting of communications from 'foreign nationals

---

[149] ibid para 11

[150] Human Rights Committee, 'General Comment 16 on the Right to Privacy' (8 April 1988) Adopted at the Thirty-second Session of the Human Rights Committee para 3

[151] (n 127)

[152] Cf. Bryce Clayton Newell, 'The Massive Metadata Machine: Liberties, Power and Mass Surveillance in the US and Europe' A Journal of Law and Policy for the Information Society 12 (forthcoming); available at < http://moritzlaw.osu.edu/students/groups/is/files/2013/11/Newell-Article.pdf>

[153] Frowein and Peukert, (n 115) 297 para 16

[154] Malone v The United Kingdom (n 133)

[155] Janis, Kay and Bradley (n 111) 452

[156] Cf. Milanovic (n 16) 68

[157] Cf. Nowak (n 35) 382–383

[158] *Liberty and Others v United Kingdom* (n 133) 51

[159] See Milanovic (n 16) 68

[160] Antonella Galetta and Paul De Hert, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance' (2012) 10 Utrecht Law Review 64

[161] A similar argument was brought by the Government of the UK in the case of *Liberty and Others v United Kingdom* (n 133) para 67

[162] ibid para 68

[163] *Liberty and Others v United Kingdom* (n 133) 60–61, 68

believed to be not on U.S. soil.'[164] The Act explicitly amended FISA[165] allowing the government an easier and a less strict surveillance conduct under the FISA framework. Section 702 allows the Attorney General together with the Director of National Intelligence to authorize targeting of 'persons reasonably believed to be located outside the United States', but does not allow to 'target' U.S. citizens. Once authorized, the information gathering may continue up to one year and permits different intelligence agencies to share the obtained information among them.[166] As for Boundless Informant, as of this writing, the legal grounds are not clear and appear to follow a praxis of warrantless monitoring.

In the UK, surveillance of communications comes under two separate law regimes. Interception of content is authorised for three or six months (depending on the purpose) by a warrant specifying an individual or premises from the Secretary of State under Part I Chapter 1 of the Regulation of Investigatory Powers Act 2000 ('RIPA'). Access to metadata is regulated under Part I Chapter 2 of RIPA, with a large number of government agencies able to self-authorise access to some of this data.[167]

As an act of Congress and a statutory law, the FAA has been published in the United States Code.[168] RIPA on its turn is an act of the UK parliament, which has been implemented by the responsible administrative department.[169] It appears that the requirement of publicity is adhered to and the pieces of legislation in question are not kept secret. A certain level of accessibility can be thus affirmed. This appears from the Guardian reports and statements of the Chair of the ISC.[170]

b. Foreseeability

The person concerned should be able to foresee the consequences following from the applicable piece of legislation for him. Thus, one important function of this requirement is to make the intrusion 'predictable'.[171] As Nardell puts it, when the citizen with whose rights the State interferes asks 'Why me?', he should be able to find an answer in the available legal arrangements that allowed the surveillance in the first place.[172]

To achieve this aim, national law must be 'sufficiently clear as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence'.[173] Also the procedures applicable in the 'examining, using and storing of intercepted material should be set out in a form which is open to public scrutiny and knowledge'.[174] This should enable every individual to determine which public authorities, mechanisms, or private individuals oversee or control their files.[175] However, the requirement of foreseeability does not provide that individuals should be able to anticipate when authorities are likely to adopt surveillance measures targeting them so that they can adapt their behaviour accordingly.[176]

Applying these criteria to the RIPA and to the US Act in question means that both acts should be particularly precise in derogating from Art. 8 (1) ECHR or Art. 17 ICCPR. Section 8 (4) RIPA stipulates that interception warrants do not have to specify a person or premises if it refers to the wiretapping of communications outside of the UK and if an authorizing certificate has been issued by a Secretary of State that also describes

---

[164] FISA Amendments Act of 2008, H.R. 6304, 110th Cong. (2008) <https://www.govtrack.us/ congress/bills/110/hr6304/text>; Ewen McAskill, 'NSA Paid Millions to Cover Prism Compliance Costs for Tech Companies' *The Guardian* (22 August 2013) <http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid>

[165] The Foreign Intelligence Surveillance Act of 1978 (FISA) was intended to curtail the NSA's ability to use its capabilities against Americans. It was passed as part of a backlash against one of the biggest controversies of that era: the unlawful surveillance by the intelligence agencies of US political activists, trade union leaders and civil rights leaders. FISA's task is to authorize the use of electronic surveillance methods against individuals who qualify as 'agents of foreign power'

[166] ibid para 206, 203

[167] 2012 Annual Report of the Interception of Communications Commissioner ("IB1/4/pp.851–920"); Cf. Brown (n 22)

[168] Cf. the official publication of the Act at <http://www.gpo.gov/fdsys/browse/collection.action?collection Code=PLAW>

[169] See the enactment of RIPA, available at the UK Statute Law Database, < http://www.legislation.gov.uk/ ukpga/2000/23/contents>

[170] Sir Malcolm Rifkind, ISC Chair: 'No, I didn't know it, nor would I have expected to any more than I would any other country's process…', Frontline Club Debate 'The Trade Off: Indiviual Privacy and National Security' *Frontline Club London* (London, 9 July 2013) <http://www.frontlineclub.com /the-trade-off-individual-privacy-and-national-security/>; 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian* (21 June 2013) <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

[171] Nowak (n 35) 383

[172] Gordon Nardell, 'Levelling up: Data Privacy and the European Court of Human Rights' in Serge Gutwirth, Yves Poullet and Paul de Hert (eds) *Data Protection in a Profiled World* (Springer 2012) 46

[173] *Malone v the United Kingdom* (Application no. 8691/79), Judgment of 2 August 1984, para. 67

[174] Ibid, para. 67

[175] HRC GC 16, ibid at fn. 142, para. 10

[176] *Malone v UK*, para. 67; *Liberty v UK*, para. 93; *Weber v Germany*, para. 93

the classes of material to be examined. This appears to be the approach by which the UK Government authorises the GCHQ to undertake automated Tempora-searches of communications that originate or terminate outside the British Isles. Consequently, RIPA's individual scope becomes rather deliberately unpredictable and indiscriminate. It does not concern a specific interference in a particular case, but rather constant and continued private life interferences, ignoring the case-by-case approach developed by the HR bodies.

The NSA framework on its turn does not require an individualized court order in order to collect information on a suspected overseas target.[177] Any foreign national outside the US can be a surveillance target under Section 702 of the FAA as long as the government's purpose is to obtain foreign intelligence.[178] An individual cannot, however, consult either the RIPA or the FAA for further criteria or clarification of the terms – a reasonable belief of being outside the US is already enough to trigger a one-year spying authorization.[179] In addition, the provisions in question do not indicate which authorities may access and control the targets' files – i.e. RIPA plainly provides a long list of public bodies permitted to use the information without defining on what ground and under what circumstances. They are thus not making the surveillance process more foreseeable, for the only foreseeable case is that no one can be sure of being exempted.

c. Compatible with the rule of law

Lastly, the law at stake itself must be compatible with the rule of law. This implies that domestic law must be able to provide effective means of legal redress against arbitrary or incongruous interference by public authorities. In this regard both the HRC and the ECtHR endorse the crucial need for independent, especially judicial supervision of approved surveillance measures.[180] In *Ekimdziev* the Court found that the Bulgarian law did not provide any independent means of review of the intelligence agency's activities after the initial authorization stage.[181] It thus failed to provide adequate guarantees against the risk of abuse.[182] The Court has come to a similar conclusion in the case of *Liberty*, where the executive enjoyed unconstrained discretion while processing surveillance data.[183] The Committee has confirmed this approach especially in the cases of telephone tapping and postal interception.[184] Volio also sees the need for an order from competent judicial authorities, in accordance with the law and procedures in force, mandated by the constitutional organs empowered to do so, and in accordance with constitutional and statutory norms.[185]

The illustrated case-law raises the bar at a reasonable level and requires the existence of a defence option for the targeted individuals. Thus the crucial question is whether foreigners enjoy some kind of rights in the monitoring process under the provision that authorized the surveillance. With regard to the GCHQ's activities, its actions outside the UK are exempt from civil and criminal liability under UK law if done pursuant to an authorization of the Secretary of State under section 7 of the Intelligence Services Act of 1994. Similarly, the protections envisioned in section 16 of RIPA which refer to material obtained under a warrant of general section 8 (4) RIPA apply only to individuals located in the British Isles at the time of the interception. It would therefore offer no protection in the present case of foreign surveillance concerns, other than to limit the period of surveillance to a maximum of six months.

With regard to the NSA, although the early adoption of FISA has brought in motion also a special court – the Foreign Intelligence Surveillance Court ('FISC') – FISA's protection and thus abuse prevention under the FAA is quite loose.[186] FISC's role is limited to reviewing the selection process and extenuation procedures that the Attorney General and the Director of National Intelligence employ to determine intelligence

---

[177] Amitai Etzioni, 'NSA - National Security v. Individual Rights' (2014) Intelligence and National Security 20; See also 'Letters to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence Leadership regarding Section 702 Congressional White Paper 'The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act', Office of the Director of National Intelligence, Washington, DC (2013), p.6, available at <http://www.dni.gov/files/documents/Ltr %20to%20HPSCI%20Chairman%20Rogers% 20and%20Ranking%20Member%20Ruppersberger_Scan.pdf>.

[178] HR 6304 (110th): FISA Amendments Act of 2008, available at <http://www.govtrack.us/congress/ bills/110/hr6304/text>

[179] Barton Gellman and Laura Poitras, 'British Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program' *The Washington Post* (6 June 2013) <http:// www.washingtonpost.com/ investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html>

[180] Cf. Milanovic (n 16) 69

[181] *Ekimdziev v Bulgaria* App no 62540/00 (ECtHR, 28 June 2007) 93

[182] ibid

[183] *Liberty and others v United Kingdom* (n 133) 64

[184] Cf. Joseph and Castan (n 85) 492; See also Concluding Observations on Lesotho, (1999) UN doc. CCPR/C/79/Add. 106, para 24

[185] See Volio (n 124) 195

[186] FISA, § 1801 (b)

targets.[187] An actual supervision during the implementation of the warrants is not officially provided for. The NSA is also overseen by Congress. But the gaps in this oversight frame have become clearer over the past few months, with many members of Congress directly objecting to Obama's persistent claim that they have signed off surveillance mandates, and insisting they had been totally unaware of the surveillance activities' extent.[188]

Finally, a curious addition to the debate is the report on the blog of the Wall Street Journal, which revealed that on several occasions NSA officers employed the agency's technical capacities to spy on their love interests.[189] The report did not present an exact number of the incidents – now known in the media as 'LOVEINT', but they all seem to have concerned overseas communications.[190] The occurrence of the mentioned incidents is a further sign of the lack of independent overview and of the urgent necessity to create such oversight.

It is important to note that these considerations relate only to the information available to the public at the moment. Accordingly, the analysis above does not claim to be exclusive, nor complete. It aims rather at showing that the already known but vague and broad statutory basis for surveillance is not sufficient, and based on what is exposed so far, incompatible with the rule of law.[191] However, although these findings are not at all unproblematic, since the present contribution does not aim at providing an in-depth analysis of the provisions' constitutionality under the respective national regimes, the remaining requirements 'legitimate aim' and 'necessity'/'non-arbitrariness' shall be considered for the sake of the argument as well.

2. Legitimate Aim

Only those aims listed under the provisions can be invoked by states, but the aims are couched in broad terms.[192] Whether invoking 'national security', 'the prevention of disorder or crime', or 'prevention of a breach of the peace', the present criterion has been rather easily satisfied. The case-law on record confirms this by showing that states have nearly always managed to convince the Court and the HRC that they were acting for a proper legitimate purpose.[193] Thus, the Human Rights bodies rarely challenge the aim referred to by states.[194]

However, the Court has established that employing secret surveillance in the fight against terrorism and espionage for the sake of national security may undermine or even destroy democracy.[195] Therefore it requires adequate and effective safeguards against abuse.[196]

3. Necessity

Let's assume for the sake of the argument that the interferences with privacy caused by foreign surveillance activities have passed all prior tests. Even so, they still must be subjected to the final control criteria of 'non-arbitrariness' and 'necessary in a democratic society'.

Already in the early cases of secret surveillance measures, the Commission and the Court in Strasbourg questioned not only whether the monitoring activities were executed in the name of national security, but also demanded that such activities fulfil the requirements of necessity.[197] In essence, the inquiry is twofold – it requires a finding of proportionality[198] while paying due regard to the precise circumstances of the given case,[199] including 'the nature, scope and duration of the measures, the grounds required for ordering them,

---

[187] Cf. Sinha (n 57) 888; Cf. 'Letter from American Civil Liberties Union to the U.S. Senate' (25 June 2008), <http://www.aclu.org/images/general/asset_upload_file902_35782.pdf>, arguing that the FISA Amendments Act 'unconstitutionally and unnecessarily permits the government to vacuum up international communications, without a connection [...] even to national security'

[188] See 'NSA Files Decoded: Edward Snowden's Surveillance Revelations Decoded' *The Guardian* (1 November 2013) <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>

[189] Siobhan Gorman, 'NSA Officers Spy on Love Interests' *Washington Wire* (23 August 2013), available at <http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/>

[190] ibid

[191] Ian Brown and Douwe Korff, 'Terrorism and the Proportionality of Internet Surveillance' (2009) 6(2) European Journal of Criminology 129

[192] See Alastair Mowbray, *Cases and Materials on the European Convention on Human Rights* (3rd edn, Oxford 2012) art. 8 (2), 591

[193] Cf. i.e. the secret collection of information about an individual in the interest of national security in *Leander v Sweden* App no 9248/81 (ECtHR, 26 March 1987) 50

[194] Fura and Klamberg (n 6) 470

[195] ibid

[196] *Klass and others v Germany* (n 133) 49–50; *Weber and Saravia v Germany* (n 133) 106, 116–118

[197] Frowein and Peukert (n 115) 296, para 16

[198] Cf. Newell (n 155) 20

[199] Nowak (n 35) 383, para 13; See also *Weber and Saravia v Germany* (n 133) 106

the authorities competent to authorise, carry out and supervise them and the kind of remedy provided by the national law'.[200]

The HRC has also followed this approach, indicating that a precise balance of the circumstances in the given case must be observed by paying regard to the principle of proportionality.[201] The Committee has further developed this line of thought in *Canepa v Canada*, where it established that 'arbitrariness extends to the reasonableness of the interference with the person's right under Art. 17 ICCPR and its compatibility with the purposes, aims and objectives of the Covenant'.[202] These criteria make it clear that privacy interferences by surveillance measures should represent the exception and not the rule in a democratic society.

a. Proportionality

When assessing the necessity of a state's conduct, the notion of proportionality is to be considered first. Even though proportionality is not explicitly mentioned in Art. 8 (2) ECHR, it is one of the main requirements that the Court considers when assessing private life intrusions.[203] In certain cases it even constitutes the final test in the Court's reasoning and its decisive point.[204] From a more empirical perspective, the very core of proportionality requires a balance of the compelling rights and interests.[205] States implementing foreign surveillance have thus the difficult task to balance between the protections of their citizens against terrorist threats while preserving also the fundamental rights of those persons suspected of terrorist activities.[206] In this regard the Court has granted state parties a margin of appreciation with regard to the actual implementation of security measures.[207] However, the implementation of the same margin of appreciation has often been scrutinized by the Court and is applied in the context of Art. 8 ECHR like a squeezebox device to which the proportionality principle adapts accordingly.[208] I.e. in *Peck* the Court stipulated that the margin of appreciation enjoyed by national authorities in the exercise of surveillance powers depends on the nature and seriousness of the interest at stake and the gravity of the interference.[209] In *Leander v Sweden* the ECtHR also emphasized that the scope of a state's margin of appreciation is related also to the particular nature of the interference involved.[210]

Now, let us apply this approach to the present scenario of foreign surveillance activities. The interference in question is the bulk data collection by the NSA programs and the respective GCHQ's practices. As was described earlier, their particular nature is quite broad, gathering indiscriminately all the communications, metadata and other raw material available in the intercepted fibre-optic cables, computers and servers. Such surveillance practices aim at collecting 'all the signals all the time'[211] and threaten the very core of the HR to privacy as stipulated in Art. 8 ECHR and Art. 17 ICCPR. The state's justification for conducting programs like PRISM, Boundless Informant or Tempora is combating sophisticated forms of terrorism and other serious national security treats, which already in the case *Klass v Germany* were affirmed as a sufficient reason for the resort to 'secret surveillance of subversive elements'.[212]

Thus, it would appear that presently states enjoy a rather broad margin of appreciation, which should be considered when assessing the proportionality between the grave interference with the fundamental human right of privacy and the measures states adopt to antagonize serious national threats.

It cannot be denied that, as a response to sophisticated terrorist threats, states need to adopt sophisticated and innovative strategies to combat these threats. This is especially so with regard to the fact that dealing with terrorists means developing capacities to prevent attacks before they even happen. Although some voices in academia argue that terrorists can be dealt with by the existing bodies and procedures like other

---

200 *Weber and Saravia v Germany* (n 133) 106

201 Nowak (n 35) 383, para 13; Further, for the emphasis on proportionality see the remarks of the British expert Higgins during the drafting of GenC 16/31, in CCPR/C/SR.749, § 26, which stipulates that interference with privacy must be at least 'reasonable in the particular circumstances'

202 *Canepa v Canada*, Comm. No. 558/1993, § 11.4, U.N. Doc. CCPR/C/59/D/558/1993

203 ibid 70

204 ibid

205 Galetta and De Hert (n 163) 69

206 Similar in Brown and Korff (n 197) 131

207 *Klass and others v Germany* (n 133) 48; *Leander v Sweden* (n 199) 59

208 Galetta and De Hert (n 163) 71

209 *Peck v the UK* App no 44647/98 (ECtHR, 28 January 2003) 77

210 *Leander v Sweden* (n 199) 59

211 Ewen McAskill and others (n 30)

212 *Klass and Others v Germany* (n 133) 48

criminals[213] their approach does not seem convincing in the counter-terrorism context. Law enforcement understands the penalisation for an offence as a deterrent against future crimes. However this traditional concept would hardly have the expected effect on terrorists - there is little ground for the assumption that those willing to commit suicide during their attack can be influenced at all; such people have nothing to lose. In other words, there appear to be some solid arguments as to why combating terrorism justifies additional and, above all, different security means than those used in dealing with 'regular' criminals on the domestic and international level.[214] These arguments do not justify any particular security means or foreign surveillance systems *per se* but, rather, support the view that public safety measures adapted or specially created to meet this threat are needed.

Now, let us apply this insight in the present surveillance context and in consideration of the available jurisprudence on the topic. The collected personal data is a powerful instrument in the hands of the security agencies, allowing them to look for evidence of serious threats. According to the leaked sources, the gathered intelligence has helped more than once to detect new techniques employed by terrorists to avoid security checks and to identify terrorists planning atrocities.[215] The data has also been employed to combat child exploitation networks and in matters of cyber defence.[216] And up until now even broad pieces of surveillance legislation have been understood as compatible and proportionate with the state's HR obligations. This approach is clearly stipulated in the case of *Weber* in which the Strasbourg judges concluded that a German law in question did not violate Art. 8 ECHR for the law was limited to cases in which there were factual indicators for suspecting persons of planning, committing or having committed certain serious criminal acts. However, in *Weber* just a small percent of telecommunications were potentially intercepted and the surveillance was restrained to a precise number of specified countries.[217] The Court was thus perfectly clear in stating that 'exploratory' or 'general' surveillance practices are not permitted by the *contested* legislation.[218] In other words, 'personal data collected for one specific purpose (i.e. countering terror threats) can only be used for another specific purpose (i.e. investigating actual offences) if the data could have been independently collected for that second purpose'.[219] No law enforcement agency should ever collect personal data 'just in case'.[220]

These points are clearly problematic in the vast (and until Snowden's revelations unimagined) scale of the NSA/GCHQ operations. So far, there are no precise criteria (i.e. for activities or offences that require specific attention by the authorities) on the basis of which surveillance may be conducted. The same applies for the duration of the surveillance, which under the Tempora, Boundless Informant and PRISM programme effectively collects data on an on-going basis. Also important in terms of the ICCPR and the ECHR is the fact that the NSA and GCHQ reportedly have direct access to the programme data of each other, for purposes going far beyond those that have been accepted by the ECtHR to justify the intrusiveness of 'strategic' surveillance systems.[221]

In light of the above-mentioned situation, limitless surveillance as in the present case is clearly out of proportion. The mere statement provided by the authorities that 'those of us who pose no threat of terrorism and do not inadvertently consort with possible terrorists should not worry that the government will track our phone or internet exchanges or that our privacy will be otherwise infringed',[222] appears out of place and neglects the core of the present issue. Where data collection takes place, individuals around the globe have to worry on an on-going basis that their communications or communications data may at some point lead to false incrimination, or (as it has already been the case) to public or private misuse of the data. Those who have reasons to be apprehensive of the data collected on them would aspire to behave as unsuspiciously as

---

213 Karen J. Greenberg, Susan Quatrone, and others, 'Terrorist Trial Report Card: September 11, 2001–September 11, 2011' The Center on Law and Security, New York University School of Law <http://www.lawandsecurity.org/Portals/0/Documents/TTRC%20Ten%20Year% 20Issue.pdf>

214 Etzioni (n 176) 9

215 Ewen McAskill and others (n 30)

216 ibid

217 *Weber and Saravia v Germany* (n 133) 110

218 *Klass and others v Germany* (n 133) 51

219 See Brown and Korff (n 197) 129

220 ibid

221 *Weber and Saravia v Germany* (n 133) 111

222 Richard Lempert, 'PRISM and Boundless Informant: Is NSA Surveillance a Threat?' (*Brookings*, 13 June 2013) <http://www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert>

possible or even refrain from communicating altogether.[223] Further, foreign surveillance activities and data retention can have an adverse effect on political activities, which would seriously impact the operation of our democratic states and thus our society.[224] It is thus clear that a balance between the conflicting rights and interests must be kept, rather than presuming that one always overtrumps the other.[225] The common good cannot be always legitimately emphasized over considerations of individual rights and personal autonomy.

Presently, there is a significant imbalance between the likely benefit of the surveillance activities and the data obtained through it, and their negative impacts, both on individuals and on society as a whole. Foreign surveillance as presently implemented by the NSA and the GCHQ is a disproportionate restriction of the privacy rights under Art. 8 ECHR and Art. 17 ICCPR.

b. Existing Safeguards

However, before making general conclusions on the NSA/GCHQ surveillance activities the available safeguards should be taken into consideration as well. This is presently of importance, for only in the cases where the ECtHR has contented itself with the existing legal safeguards, has it ruled out a violation of Art. 8(1) ECHR. Thus, following its lead, after examining the proportionality of foreign surveillance measures, a holistic overall assessment of the existing safeguards against abuse must be made. Such adequate and effective safeguards are required regardless of the monitoring system's structure[226] and should be set out in statutory law.[227] Further, following the notion of proportionality, the required remedy must be tailored to the legitimacy of the state's power to interfere with the right rather than the right of the individual.[228] The same remedy must be available to anyone with an arguable claim.

In the present case, the available safeguards raise some serious doubts. Some of the problems are already briefly introduced above;[229] some will be addressed for the first time.

To begin with, a large part of the applicable terms is hidden from public view, making it impossible to ascertain whether the existing safeguards achieve their aim. Also, it is difficult to see how this situation is compatible with the UK's or the US' obligations to protect the privacy of those under their jurisdiction.

The available procedures, although considered an improvement[230] especially with regard to some of the points defeated by the ECtHR in the UK-related cases, do not bear up the necessary protective threshold required in extraterritorial surveillance procedures. In view of the collected data, there are no known clear rules limiting its use and disclosure or its sharing with other intelligence agencies, including the agencies of the other 'Five Eyes' states. So far, there are also no known provisions that ensure that collected data is not unduly retained when it is no longer needed or relevant. In this regard, both intelligence agencies have been reluctant to provide the public with more details on the matter. Whether the data is actually deleted after the period of two or five years cannot be ascertained and the agencies' argument they would not have the technical capacities to keep it after this time frame is simply not plausible anymore.

Further, because the online services of the private companies cooperating with the NSA are popular globally, and are covered by US law, their users worldwide can expect their personal data to be open to inspection by the NSA with no expectation of legal protection, if the person is outside the US.[231] More controversially, the FAA of 2008 conferred retroactive immunity to telecom companies that had been forwarding data to the NSA without the involvement of the FISC.[232] The law requires annual reports from the Attorney General and the Director of the National Intelligence to the FISC, which has the last word on approving the government's

---

[223] Patrick Breyer, 'Telecoms data retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) 11 (3) European Law Journal 371

[224] ibid

[225] ibid

[226] *Klass and others v Germany* (n 133) 50

[227] *Shimovolos v Russia* App no 30194/09 (ECtHR, 21 June 2011) 68

[228] Harris, O'Boyle, Bates and others (n 112) 423

[229] ibid 32

[230] Richard Stone, *Textbook on Civil Liberties and Human Rights* (9th edn, Oxford, 2012) 254

[231] Andrew Clement 418

[232] Cf. Sinha (n 57) 886; See also Kit Bond, 'FISA Amendments Act of 2008' *The Wall Street Journal* (New York City, 19 June 2008) <http://online.wsj.com/article/SB121391360949290049.html> (noting this liability protection extends up until 'the President's Terrorist Surveillance Program was brought under the FISA Court'; Paul Kane, 'House Passes Spy Bill, Senate Expected to Follow' *Washington Post* (Washington, D.C., 21 June 2008) <http://www.washingtonpost.com/wpdyn/content/story/2008/06/20/ST2008062001087.html> (not-ing that immunity depends on showing 'written assurance from the Bush administration that the spying was legal')

surveillance provisions and its targeting of foreigners outside the US.[233] However, the same regulation gives the Director of National Intelligence and the Attorney General joint power to issue extensive, yearlong warrants for targeting foreign individuals or groups,[234] obviating the FISC's warrant approval.

Walton wrote that the 'government has compounded its noncompliance with the court's orders by repeatedly submitting inaccurate descriptions of the alert list process', and that 'It has finally come to light that the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses' the phone call data.[235]

Further, there are no real safeguards against abuse, with the current oversight regimes having been shown to be unable to check the growth of NSA or GCHQ employees and contractors who use the monitoring systems to spy on and control their own personal affairs. Frequent over-collection of data by government officials is also a common phenomenon.[236]

Stone particularly points out the vagueness of the grounds for some of the surveillance procedures and the lack of independent supervision[237] - these policies and procedures are not published and not subjected to Parliamentary or public democratic scrutiny. For some of the specific targeted surveillance measures conducted by the GCHQ there is no involvement of the Surveillance Commissioners.[238] GCHQ's compliance with the certificates is subjected to the agency's own oversight and the results of those audits are confidential as well. Also, although an individual (at least one being on UK soil) willing to file a complaint can turn to the Tribunal established under RIPA 2000, another route for remedy is not foreseen and the work of the RIPA Tribunal itself is not under scrutiny by any other institution. However, the complaint before the Tribunal concerns only search operations or targeted surveillance activities. The generalised warranting process that authorizes the Tempora programme does not qualify as such.

At the very least, more information about how the governments execute the programs is needed.

These technologies have the potential to enable small groups of people to restrict the freedom and to control the perception of a great numbers of individuals.[239] The first signals that during the last presidential campaign Barak Obama has used surveillance technology to reconstruct the behaviour of potential voters in order to comprehend and address their values in his designations are already public. While catching up on the political program of a candidate running for office is the fair choice of the electorate and a democratic right, this is certainly not the case when the same candidate manipulates you by monitoring your activities and tracking your interests. The storage and use of large amounts of intelligence (including communications' metadata) can and already greatly impacts the relationships between governments and their citizens.[240] Information can (and does) provide and facilitate power.[241]

The findings illustrated above bring some serious doubts with regards to the legality of the NSA/GCHQ surveillance programs. The present analysis has highlighted a number of ways in which the foreign surveillance programs seem both unlawful and arbitrary and accordingly out of proportion to the privacy rights they interfere with. Although additional and more concrete information is further needed to present this complicated argument in bullet-proved manner, at a minimum we face the frightening prospects that the US-UK surveillance ensemble is systematically and massively violating the human right to privacy under Art. 8 ECHR and Art. 17 ICCPR. These interferences further suggest that the surveillance legal framework both in Europe and across the Atlantic needs urgent and substantial revision in order to be brought in line with the demands of the ECHR and the ICCPR. Whilst the tensions described above cannot be simply eradicated, they can be managed sufficiently through oversight mechanisms that do permit public scrutiny.

---

233 50 U.S.C.S. § 1881a (2008)

234 See Human Rights Watch, 'Privacy and Civil Liberties Oversight Board, Comments of Human Rights Watch' (2013) <http://www.hrw.org/sites/default/files/related_material/Comment%20HRW%20PCLOB%20Final%208-1-13_0.pdf>

235 Scott Shane, 'Court Upbraided NSA on its Use of Call-Log Data' *The New York Times* (New York City, 10 September 2013) <http://www.nytimes.com/2013/09/11/us/court-upbraided-nsa-on-its-use-of-call-log-data.html?page wanted¼all>

236 Sinha (n 57) 944

237 ibid

238 McAskill and others (n 30)

239 Lempert (n 230)

240 Brown and Korff (n 197) 131

241 ibid

III. Outlook

A. Additional Safeguards

Based on what has been disclosed and analysed so far, the surveillance practices of the NSA and GCHQ require the urgent development of new procedural obligations in order to secure online and communication privacy from state intrusions. Many voices in academia, aware of what is at stake, advocate in their recent contributions similar reforms or improvements and address the need for transparency on the domestic level in the first place.

The frameworks of collection and access to personal data must be transparent. In the area of law enforcement, data protocols should be mandatory and available to those whose information is processed.[242] The records of the data should be kept only within the period established by law and the individuals concerned should have the opportunity to verify, if needed, that no data concerning them is available in the respective system.

As for intelligence gathering, there must be similar transparency of data access for public security, unless transparency presents a danger for the public safety.[243] This immediately leads us to the next safeguard matter – what authority should decide on the issues of public safety and whether these trump the public's right to access the information? What has become clear from the present case study is that the available legal framework has failed to provide for an independent body of experts that monitors the agencies' activities. The determination of a situation as a danger for the public's safety should therefore be made by an authority that is independent from the executive.[244] The executive should not be able to control the dissemination of access orders for the simple fact that this would otherwise allow for selective disclosure to distort the public's understanding of the government's behaviour, or for at least a quite obvious temptation for the government to control the disclosure process of its activities.[245]

More consideration should be also given to civic bodies and the enhancement of their role. As a separate authority, they are not part of the government but the independent civilian board could help oversight the implementation of the surveillance programs by conducting regular reviews of the projects and their authorization. The board would present reports on regular basis that would verify whether or not state agencies have gathered data for political reasons instead of pursuing security concerns and other legitimate legal goals. However, since revealing intelligence objectives and related information is a rather sensitive issue that needs a precise preparation before it can be simply published in a report, instead of exposing detailed case studies, the civilian review board could provide its investigation in the form of statistics.

A further strengthening of the public participation could be introduced through the appointment of public advocates to the FISC and the RIPA Tribunal proceedings that would represent the interests of both US/UK persons and non-nationals located abroad. A public advocate would strengthen the proceedings by ensuring that the respective judicial bodies receive the arguments of the other side as well. This would be a valuable tool to promote confidence in the legitimacy of the surveillance programs by showing at the national and international level that individual's concerns are heard and considered. Such an approach could also serve as an *ex ante* check on the governments, encouraging them to adopt those criteria that could withstand subsequent scrutiny and criticism. In his speech in January this year, President Obama considered a similar approach by proposing a panel of independent lawyers who could participate in important FISC cases. However, further institutionalization of this role would be crucial in order to establish a body that does not only keep up the appearances and silences the disputants. A public advocate should scrutinize and when necessary challenge the NSA's or the GCHQ's targeting criteria on a regular basis.[246]

A further point for consideration is the behaviour of government officials. The legal framework authorizing the surveillance must provide for personal and general liability in the case of over – reaching[247] and abusive exploitation of the intelligence programs. Further, when a senior government functionary admits to cheating a public oversight body, the failure to sanction the latter transmits a powerful message of tolerance

---

[242] Reidenberg (n 2) 28

[243] ibid 29

[244] ibid

[245] In the recent US context, only 2 FISA court orders have been released and they have been released only in a form heavily redacted by the US government. Because this is such a highly selective disclosure, the public does not know the true nature of the FISA court's activities and decisions

[246] For more detail on such proposals, see Marty Lederman and Steve Vladeck, 'The Constitutionality of a FISA 'Special Advocate'' (4 November 2013) <http://justsecurity.org/2013/11/04/fisa-special-advocate- constitution/>

[247] Reidenberg (n 2) 1

for wrongful intrusions into ordinary people's lives and abusive state actions.[248] In this context, i.e. internal disciplinary measures as in the case of 'LOVEINT' are clearly not sufficient to discourage the misuse of the data surveillance personnel has access to.

However, the question of the framework's transparency and its capacity of providing effective legal safeguards concerns the international institutions as well. A strong example has been given by the eagerness of the ECtHR to adapt Art. 8 ECHR to new security threats and technological challenges. It can only be hoped that the Court shall deliver a further benchmark in the case of *Big Brother v the UK* that would provide the necessary guidance for the future assessment of surveillance programs implemented by the GCHQ, the NSA or other intelligence agencies. As for the ICCPR, the HRC should not further postpone considering Art. 17 ICCPR in the new surveillance context. Right now General Comment 16 on the right of privacy, which is not longer than two pages and over twenty-five years old, is an outdated tool that lacks important details, and does not refer to surveillance practices that are widely employed around the world today.[249] If the right to privacy is to be preserved, not only the law but also its institutions must respond correspondingly. Right now, some affirmative guidance from the Committee is essential for the settlement of the limits on foreign surveillance. Otherwise, it becomes much easier for states to ignore their human rights responsibility when they can claim obscurity of the applicable law.

B. Conclusion

In the first place, after setting the scene and illustrating the problems of foreign surveillance, this contribution illustrated the gaps in the argumentation of the US government concerning the extraterritorial applicability of the ICCPR. While the US position conveniently matches their surveillance behaviour outside the national borders, it relies on dubious interpretation of discussions during the drafting phase of the Covenant. The US position regarding Art. 2 (1) ICCPR is thus not tenable under international law. This finding is of a great value for the present investigation because it affirmed the applicability of the existing legal framework and allowed for the submission of the NSA activities under the ICCPR. The use of human rights as a regulatory framework makes sense precisely because of the fact that surveillance measures are now deployed against masses of ordinary people both at home and abroad, rather than simply against the agents of foreign governments who could otherwise be left to their own devices.[250] State parties to the human rights treaties neglecting their applicability on foreign surveillance activities will not be able to sustain their positions in the long term. This has become clear especially by the fact that both the HRC and the ECtHR have already developed some valuable criteria for the assessment of state surveillance measures, which are not easy to omit.

Further, with regard to the interests protected under Art. 8 ECHR and Art. 17 ICCPR, the present contribution has come to the conclusion that the surveillance activities conducted by the NSA and the GCHQ pose a serious threat to and interfere with the individual's privacy rights.

These programmes involve countless interferences with privacy rights. These interferences come partly conditioned by states' responses to terrorist threats. They feel urged to take drastic actions, even if this implies a deviation from their usual human rights obligations applicable in 'ordinary' times.[251] Yet, regulations established under a state of emergency in order to address momentary threats must remain within the legal framework and not undermine fundamental democratic values. Meanwhile, the 'war on terror' has been going on for more than thirteen years with no end in sight, and it is now clear that the threat of terrorism is still very real.[252] Thus, although undeniably more then serious national interests are at stake, the current surveillance practice should be redesigned and founded on legitimate grounds in accordance with the respective national laws and international law. For the law authorizing the NSA or GCHQ's programs ignores various safeguarding requirements as indicated under Art. 8 (2) ECHR and Art. 17 (1) ICCPR. A measure of surveillance is not 'necessary in a democratic society' unless shown to respond to a 'pressing social need', supported by 'relevant and sufficient reasons'. No 'special' or beneficiary rules can or should be used in order to authorize foreign surveillance measures.

---

[248] See the point made by Reidenberg (n 2) 29; See also Hearing on Warrantless Geolocation Surveillance and National Security Agency Tracking before the Senate Intelligence Committee, 113th Cong., 1st Session 12 March 2013, (testimony of NSA Director Clapper stating that NSA does not collect data on hundreds of millions of Americans), available at <https://www.youtube.com/watch?v=QwiUVUJmGjs&feature=youtu. be&t=6m9s>

[249] Cf. Sinha (n 57) 945

[250] Milanovic (n 16) 74

[251] Brown and Korff (n 197)120

[252] ibid

What does this all mean? It implies that our society is developing in a profoundly undemocratic way.[253] And we have already seen that these surveillance practices have managed to create a new sense of 'urgency in defence of privacy',[254] a sense of fear and distrust, doubting our next-door neighbours instead of uniting our efforts in a democratic and legitimate way. What we need to keep in mind is that 'few things would provide a more gratifying victory to the terrorist than for our countries to undermine their traditional freedoms in the very process of countering the enemies of those freedoms.'[255] Otherwise we are indeed just giving up freedom without gaining more security in return.[256] This is why further reforms are essential in order to remove the already existing barriers between the US, the UK and the rest of the world. In this regard, it is important to note that this contribution's argument did not aim at persuading the reader that the surveillance practices should be cancelled *per se,* or that foreign surveillance is ineffective or unjustifiable. Rather, it attempted to draw the attention to the need to focus on the source of danger and that intelligence agencies should operate in accordance with basic concepts of the rule of law.[257]

[253] Brown and Korff (n 197) 132
[254] See Fried (n 121) 475
[255] 882 PARL. DEB., H.C. (5th ser.) (Nov. 29, 1974) 634 (Roy Jenkins)
[256] Brown and Korff (n 197) 131
[257] See the point made by Nardell (n 176) 52

Bibliography

Bielefeld H, Philosophical and Historical Foundation of Human Rights in Catarina Krause and Martin Scheinin (eds), *International Protection of Human Rights: A Textbook* (Sastamala 2012) 3–18

Breyer P, 'Telecoms data retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR' (2005) European Law Journal 365–375 DOI: http://dx.doi.org/10.1111/j.1468-0386.2005.00264.x

Brown I, Expert Witness Statement for Big Brother Watch and Others Re: Large-Scale Internet Surveillance by the UK (September 27, 2013), Application No. 58170/13 to the European Court of Human Rights <http://ssrn.com/abstract=2336609>

Brown I and Korff D, 'Terrorism and the Proportionality of Internet Surveillance' (2009) 6 (2) European Journal of Criminology 119–134

Buergenthal T, 'To Respect and to Ensure: State Obligations and Permissible Derogations' in Louis Henkin (ed), *The International Bill of Rights: The Covenant on Civil and Political Rights* (Columbia University Press 1981) 72–91

Clark D and Landau S, 'Untangling Attribution' (2011) 2 Harvard National Security Journal 323–352

Dennis M, 'Application of Human Rights Treaties Extraterritorially During Times of Armed Conflict and Military Occupation' (2005) American Journal of International Law 119–141

Dworkin R, *Is Democracy Possible Here?: Principles for a New Political Debate* (Princeton University Press 2006)

Etzioni A, 'NSA - National Security v. Individual Rights' (2014) Intelligence and National Security 1–37

Fernández-Sánchez P A, 'The Scope of Obligations under the European Convention of Human Rights' in Javier García Roca and Pablo Santolaya (eds), *Europe of Right: A Compendium on the European Convention of Human Rights* (Leiden/Boston 2012) 27–40

Fried C, 'Privacy' (1968) 77 Yale Law Journal 475–493

Frowein J and Peukert W, Europäische Menschenrechtskonvention, 3. Auflage, Engel Verlag 2009

Fura E and Klamberg M, 'The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA' in *Freedom of Expression: Essays in honour of Nicolas Bratza* (Wolf Legal Publishers 2012) 463–481

Galetta A and De Hert P, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance' (2012) 10 Utrecht Law Review 55–75

Grabenwarter C, *The European Convention on Human Rights: Commentary* (OUP 2014)

Greenberg K J, Quatrone S, and others, 'Terrorist Trial Report Card: September 11, 2001–September 11, 2011' The Center on Law and Security, New York University School of Law <http://www.lawandsecurity.org/Portals/0/Documents/TTRC%20Ten%20Year%20Issue.pdf>

Harris D, O'Boyle M, Bates E and others, *Law of the European Convention on Human Rights* (2nd edn, Oxford 2007)

De Hert P and Boehm F, 'The Rights of Notification after Surveillance is over: Ready for Recognition?', in Jacque Bus, Malcolm Crompton and other, *Digital Enlightment Yearbook 2012* 19–40

Janis M W, Kay R S and Bradley A W, *European Human Rights Law: Text and Materials* (3rd edn, Oxford 2008)

Joseph S, Schultz J and Castan M, *The International Covenant on Civil and Political Rights: Cases, Materials and Commentary* (2nd edn, Oxford 2004)

Lawson R, 'The European Convention on Human Rights' in Catarina Krause and Martin Scheinin, *International Protection of Human Rights: A Textbook* (Sastamala 2012 423–462

Lawson R, 'Life after Bankovic: On the Extraterritorial Application of the European Convention on Human Rights', in Fons Coomans and Menno Kamminga, *Extraterritorial Application of Human Rights Treaties* (Intersentia 2004) 83–123

Margulies P, 'The NSA in Global Perspective: Surveillance, Human Rights and International Counterterrorism (2014) 82 Fordham Law Review 2137–2167

Ma Z and others, 'Towards a Multidisciplinary Framework to Include Privacy in the Design of Video Surveillance Systems' in *Privacy Technologies and Policy* (2014) 101–116

McGoldrick M, 'Extraterritorial Application of the International Covenant on Civil and Political Rights' in Fons Coomans and Menno T. Kamminga, *Extraterritorial Application of Human Rights Treaties* (Oxford 2004) 41–71

Milanovic M, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (March 31, 2014), Harvard International Law Journal, Forthcoming, <http://ssrn.com/abstract=2418485>

Mowbray A, *Cases, Materials and Commentary on the European Convention on Human Rights* (3rd edn, Oxford 2012)

Nardell G, 'Levelling up: Data Privacy and the European Court of Human Rights' Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer 2012) 43–51

Newell B C, 'The Massive Metadata Machine: Liberties, Power and Mass Surveillance in the US and Europe', A Journal of Law and Policy for the Information Society, Forthcoming, <http://moritzlaw.osu.edu/students/groups/is/files/2013 /11/Newell-Article.pdf>

Nowak M, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (2nd revised edn, 2005)

Reidenberg J R, 'The Data Surveillance State in the United States and Europe' (November 2, 2013), Wake Forest Law Review, Forthcoming, <http://ssrn.com/abstract=2349269>

Rodley N, 'Civil and Political Rights' Catarina Krause and Martin Scheinin, *International Protection of Human Rights: A Textbook* (2nd edn, Sastamala 2012) 105–129

Scheinin M, 'Extraterritorial Effect of the International Covenant on Civil and Political Rights' in Fons Coomans and Menno Kamminga, *Extraterritorial Application of Human Rights Treaties* (Intersentia 2004) 73–81

Scheinin M, 'Characteristics of Human Rights Norms' Catarina Krause and Martin Scheinin, *International Protection of Human Rights: A Textbook* (2nd edn, Sastamala 2012) 19–38

Schiedermair S, 'Data Protection – Is There a Bridge across the Atlantic?' Dieter Dörr and Russell L. Weaver, *The Right to Privacy in the Light of Media Convergence Perspectives from Three Continents* (Berlin/Boston 2012) 357–373

Shaw M N, *International Law* (6th edn, Cambridge 2008)

Sinha A, 'NSA Surveillance since 9/11 and the Human Right to Privacy' 59 Loyola Law Review 861–946

Stone R, *Textbook on Civil Liberties and Human Rights* (9th edn, Oxford 2012)

Van Schaack B, 'The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change' (2014) 90 International Law 20–65

Volio F, 'Legal Personality, Privacy and the Family' in Louis Henkin (ed), *The International Bill of Rights: The Covenant on Civil and Political Rights* (Columbia University Press 1981) 185–208

Warren S D and Brandeis L D, 'The Right to Privacy' (1980) 4 Harvard Law Review 193–220

Westin A F, *Privacy and Freedom* (Athenaeum, New York 1967)

Wilborn E, 'Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace' (1998) 32 Georgia Law Review 825–888

How to cite this article: 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, DOI: http://dx.doi.org/10.5334/ujiel.cr

Published: 27 February 2015

]u[*Utrecht Journal of International and European Law* is a peer-reviewed open access journal published by Ubiquity Press.

OPEN ACCESS