ADDIS ABABA UNIVERSITY

FACULTY OF LAW

SCHOOL OF GRADUATE STUDIES

International and Regional Framework for Governing Foreign Digital Surveillance in Africa

Thesis Submitted in Partial Fulfillment of Master of Laws Degree (LL.M) in Public International Law at Addis Ababa University

-By-

Nati Tesfu

- Advisor -

Takele Soboka Bulto (PhD)

March, 2017

Declaration

I, undersigned, declare that this thesis is my original work and has not been presented for a degree in any other university and that all sources of materials used for the thesis have been duly acknowledged.

_____

Nati Tesfu

March, 2017

Conformation

This thesis is submitted for examination with my approval as an advisor to the candidate.

_____

Takele Soboka Bulto (PhD)

March, 2017

This thesis is submitted to the Faculty of Law and to the School of Graduate Studies of Addis Ababa University in fulfillment of all requirements for the degree of masters in Public International Law.

Title of Thesis: **International and Regional Framework for Governing Foreign Digital Surveillance in Africa**

Author: Nati Tesfu

Date: March, 2017

Approved by Board of Examiners:

Takele S. (PhD)	.....	.....
Advisor	Signature	Date
Mekete B. (Asso. Prof.)	…….....	.....
Examiner	Signature	Date
Mizanie A. (PhD)	…….....	.....
Examiner	Signature	Date

Acknowledgment

Above all I would like to thank GOD for giving me the patience and perseverance to achieve this work. My gratitude also goes to my family, friends and classmates who gave up their precious time to help me think through and put together this thesis. Special recognition must be given to my mother and brothers for their unwavering support.

I also would like to express my deep appreciation for my advisor Dr Takele for his continued input and encouragement. It was a privilege to work under his guidance. Finally I feel greatly indebted to all who gave a helping hand and provided advice to the accomplishment of this paper. Without you this would not have been possible.

Abstract

In today's modernized world the use of vast technological innovations have made it easier for individual to conduct their day to day lives. These advances, although necessary, do bring with them a rise in the surveillance capabilities of states. This combined with the threats posed by transnational crimes and the growing phenomenon of terrorism have put greater pressure on states to insure national security interests through electronic surveillance techniques once seen as unimaginable. The emergence of these privacy intrusive capabilities have also made it easier to conduct surveillance on national and foreigners alike, putting in to question of how states can regulate the right to privacy of foreign nationals.

Due to the extraterritorial nature of this form of digital surveillance, international and regional human rights laws have struggled to find a lasting solution to deal with the issue. However, recently significant advancements have been made both in the international and European human rights jurisprudence dealing with this issue of foreign digital surveillance (FDS). In 2014, African also had its own landmark agreement on data protection possibly having progressive impacts on the regulation of FDS. However, it continues to be debatable as to whether this agreement alone can govern foreign digital surveillance programs in Africa.

With this in mind the paper assesses the potential of governing FDS in Africa by exploiting the existing African, international and other regional frameworks of human rights and data protection within the context of the right to privacy. The analysis will start by identifying how the concept of privacy is viewed and its relation with foreign digital surveillance programs. Then, the paper will examine the extraterritorial application of human right treaties by studying models, approaches and case law in international and regional human rights law. This investigation will highlight how international human law is currently being applied to foreign digital surveillance programs. The research will also describe the adequacy and gaps of the existing African regional human rights and data protection framework in dealing with foreign digital surveillance. Based on this analysis this paper concludes that a lasting framework for governing foreign digital surveillance in African is to be found by utilizing the existing data and human rights protection frameworks in the continent while also drawing lessons and inspirations from other more advanced international and regional human right legal frameworks.

List of Acronyms

ACHPR	African Charter on Human and Peoples' Rights
ACHR	American Convention on Human Rights
ADIRF	African Declaration on Internet Rights and Freedoms
AU	African Union
AUCSDP	African Union Cyber Security and Data Protection Convention
CEMAC	Economic and Monetary Community of Central Africa
EAC	East African Community
ECCAS	Economic Community of Central African States
ECJ	European Union Court of Justice
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms on Human Rights
ECOWAS	Economic Community of West African states
ECtHR	European Court of Human Rights
FDS	Foreign Digital Surveillance
GCHQ	United Kingdom Government Communications Headquarters
HRC	United Nations Human Rights Council
IACHR	Inter-American Commission on Human Rights
ICCPR	International Convention on Civil and Political Rights
IPAHRC	International Principles on the Application of Human Rights to Communications Surveillance
NATO	North Atlantic Treaty Organization
NPA	National Protection Authority

NSA	United States of America National Security Agency
OHCHR	Office of the High Commissioner for Human Rights
RECs	Regional Economic Communities
SADC	Southern African Development Community
UDHR	Universal Declaration of Human Rights
SRP	United Nations Special Rapporteur on the Right to Privacy
UK	United Kingdom
UN	United Nations
US	United States of America
VCLT	Vienna Convention on the Law of Treaties

Table of Contents

Chapter 5: Conclusion and Recommendations

Chapter One:

Introduction

1.1. Background of the Study

On June 2013 there was a revelation made by a British newspaper, the Guardian, detailing the nature and capabilities of states like the U.S. (through its National Security Agency or NSA) and the United Kingdom (through its Government Communications Headquarters or GCHQ) to conduct digital mass surveillance.[1] This revelation sparked a debate as to the regulation of surveillance technology in balancing out the right to privacy of individuals and the national security interests of states.[2] In order to govern these human rights concerns progress has been made indicating that international human rights law applies to cyberspace and cyber-related activities such as foreign digital surveillance.[3] However, the content and scope of application of international human rights law to cyberspace has not been settled.

Given the act and forms of surveillance differ, for the purpose of this research the term 'Foreign Digital Surveillance' is defined as a state sponsored act done by encompassing data collection and storage practices, processing, transfer of the gathered data to a third party and interception of electronic or other kinds of communications.[4]

In other words FDS is targeted at the information that either passes through the Surveillance State in the form of 'Transnational surveillance' or is stored entirely overseas in the form of 'Extraterritorial surveillance'. Accordingly, this paper seeks to assess the existing progresses made in international human rights law towards the issue of FDS and apply them to the existing African human rights and data protection frameworks.

---

[1] See generally, Paul Farrell, "History of 5-Eyes—Explainer", The Guardian, (Dec. 2, 2013), (http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.); last visited on June 12, 2016.

[2] 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", Utrecht Journal of International and European Law, Vol 31, (2015), p. 104-130.

[3] Human Rights Council, "The Promotion, Prot. and Enjoyment of Human Rights on the Internet", U.N. Doc. A/HRC/20/L.13, (June 29, 2012), ("The same rights that people have offline must also be protected online"); Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; See also discussion in Ashley Deeks, "An International Framework For Surveillance", Virginia Journal Of International Law, Vol 55:2, (2015).

[4] Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age", Harvard International Law Journals, Vol 56, (2015), p. 81-146.

1.2. Statement of the Problem

The modern concept of FDS is understood to be a form of peacetime espionage by one state of the communications of another state's officials or citizens, when those communications take place partly or entirely outside the surveillance state's territory; by the use of electronic means including cyber-monitoring, telecommunications monitoring, satellites, or other related technologies.[5] This transnational and extraterritorial action of states has a significant impact on how foreigners enjoy their right to privacy. Additionally, significant technological advancements in how states conduct surveillance dose also warranted the need to broaden the protection of privacy extraterritorially.[6] However, the existing international and regional human rights legal frameworks have been slow to address this ever changing way of how a state can conduct foreign surveillance.[7] With this in mind the researcher seeks to assess the possible remedies available for foreign nationals in international and regional human rights frameworks and apply them to the African regional context.

1.3. Objectives and Purpose of the Research

1.3.1. General Objectives

This study has the following general objectives:

- Investigating what the right to privacy entails in international human rights law
- Discover the extent to which international human rights law has addressed the issue of FDS.
- Asses the feasibility of extraterritorial application of human rights norms such as the right to privacy and its relevance to FDS.
- Look at the existing frameworks in the African regional context which could possibly govern FDS and asses its gaps.

[5] Deeks, Supra note 3, p. 299.

[6] See generally, Report on the Existence of a Global System for the Interception of Private and Commercial Communication, European Parliament Document. no 2001/2098, (July 11, 2001); See also Tara Davenport, "Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis", Cath. U. J. L. & Tech, Vol 24, (2015); See also Glenn Greenwald & Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others", The Guardian , (June 7, 2013).

[7] See generally, A. John Radsan, "The Unresolved Equation of Espionage and International Law", Michigan Journal of International law, Vol 28, (2007), p.595-597; See also Will Thomas DeVries, "Protecting Privacy in the Digital Age", Berkeley Tech Law Journal, Vol 18, (2003), p. 283, 291-368.

- Explore ways to apply international and other regional human rights framework approaches to privacy in order to fill the gap in African regional human rights framework governing FDS.

1.3.2. Specific Objectives

This study has the following specific objectives:

- Assessing the role of citizenship in determining the right to privacy of individuals.
- Examining the ICCPR, ECHR and UDHR and the VLCT rules of treaty investigation in regards to the extraterritorial application of human right treaties.
- Investigating the potential and adequacy of applying international and regional human rights instruments to FDS programs.
- Exploring the African regional human rights and African data protection frameworks which could possibly govern FDS.
- Providing concrete mechanisms in international human rights law jurisprudence, resolutions and case law as complimentary tools to govern privacy rights and FDS in Africa.

1.4. Research Questions

On the basis of the problems and objective of the study, the research question of this research paper is:

- How to deal with FDS in Africa by utilizing the existing international and regional frameworks of human rights and data protection within the context of the right to privacy?

To address this, the following sub questions will be considered

- ✓ What is the nature and substance of the right to privacy and how it is viewed in current international human rights law instruments?
- ✓ Is there a nexus established between the right to privacy and the documented FDS programs and communication interception systems?

- ✓ How are the aspects of applicability and legality of FDS programs discussed in international human rights instruments such as the ICCPR, ECHR and UDHR?
- ✓ Can the extraterritorial application of the right to privacy in these international law instruments be a remedy in dealing with FDS and what could be the possible form, critique and feasibility of a global right to privacy as a remedy to FDS?
- ✓ Dose the existing African regional human rights and data protection framework and deal with the issues of FDS? If not can extraterritorial application of the right to privacy in international and other regional human rights frameworks fill this gap?

1.5. Literature Review

Scholars have suggested that the international human rights regime can be an outlet to establish a viable framework governing actions of state imposed surveillance.[8] There have also been some developments especially in the sphere of international human rights law to indicate that the international community is trying to regulate FDS. This is evident in the recent 2014 report by the Office of the High Commissioner for Human Rights (OHCHR).[9] This OHCHR report identifies that surveillance should be done in a manner that is not arbitrary and unlawful. Additionally, international and regional case law concerning surveillance has been growing especially in the European human rights jurisprudence.[10] These developments are making those surveillance techniques that don't pass the parameters of legality, necessity, and proportionality contrary to human right standards.[11] Although the above advances suggest a positive trend for protecting privacy in a digital age there is still no internationally agreed framework specifically tailored towards FDS.

[8] See, Milanovic, Supra note 4; See also Georgieva , Supra note 2; See also Chantal Khalil, "Thinking Intelligently About Intelligence: A Model Global Framework Protecting Privacy", George Washington International Law Review, Vol 47, (2015); See also Russell Buchan, "The International Legal Regulation of State-Sponsored Cyber Espionage, International Cyber Norms: Legal, Policy & Industry Perspectives", NATO CCD COE Publications, (2016), p. 65.; See also Binoy Kampmark, "Restraining the Surveillance State: A Global Right to Privacy", Journal of Global Faultlines, Vol 2, (2014), p. 1.

[9] Office of the High Comm'r for Human Rights, "The Right to Privacy in the Digital Age: Report of the OHCHR", U.N. Doc. A/HRC/27/37, (June 30, 2014). [hereinafter OHCHR Report]

[10] Federico Fabbrini, "Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the United States", Harvard International Law Journal, Vol 28, (2015).

[11] Id, p. 74.

This lack of an appropriate framework to deal with FDS has also impacted the African regional context.[12] While in comparison to others the African states do not possess vast surveillance capabilities, the need for a viable regional framework to govern FDS has impacts on human rights, trade and regulation of 'Meta data'.[13] Therefore to ensure a more feasible solution, the following four categories of authors purpose different approaches for lasting mechanism both in international and African regional human rights law.

The first category include the work of Chantal Kahlil who proposes that the international community should create a convention that establishes a process for intelligence collection providing safeguards and oversight mechanisms to protect privacy interests.[14] However, in doing so the article fails to show clearly what substance and outline this universal convention should entail and does not put enough emphasis on unwillingness of states to engage in such debate. It also does not specify which area of international law should be considered as a bench mark (for e.g. International human rights law) rather tries to give a general description on the frameworks of self-defense, state sovereignty, customary international law and international human rights laws.

The second category of authors advocate for using tools of already established norms and practice of states to deal with the issue of FDS. To this end, Ashley Deeks ascertains the idea that international law must strike a middle ground between those "unduly optimistic in predicting that regulatory pressures will subside in short order, and those … who seem confident that states quickly will retreat from foreign electronic surveillance to a posture that is far more protective of individual privacy".[15] However, Deeks does not asses the feasibility and the nature of existing international human rights framework which has made significant progress on the issue of FDS and is heavily reliant on existing norms.

The third groups of authors advices on either a universal or extraterritorial applications of the right to privacy to deal with foreign surveillance. This research also follows this format proposed by authors such as Milanovic and Georgieva.

[12] Arthur Gwagwa & Anna Wilton ," Protecting the right to privacy in Africa in the digital age", Paper written as part of the Global Surveillance & Safeguards Project, by Privacy International, IDRC, Canada and their African partners, first published at the Africa Internet Governance Summit, Djibouti, (31 May 2014).
[13] Ibid.
[14] Khalil, Supra note 8, p. 919.
[15] Deeks, Supra note 3, p. 296.

Milanovic takes the stand that a real discussion to be had is not on the threshold question of applicability but on the substance of an extraterritorial right to privacy.[16] This author looks at how the legality of FDS programs should be debated and assessed within the existing framework of international human rights law. Although the article is quite detailed in its assessment of legality it does not take in to full consideration the recent developments (such as the report made by Office of the High Commissioner for Human Rights)[17] and further developments in case law.[18]

The article by Georgieva discuss the Right to privacy and Foreign Surveillance under the NSA and the GCHQ, detailing its Compatibility with article 17 International Convention on Civil and Political Rights (ICCPR) and article 8 European Convention on Human Rights (ECHR).[19] The primary focus of this article is also the assessment of applicability and legality of right to privacy vis-à-vis foreign surveillance. While it strictly analyzes issues of legality and applicability, the possible shortcomings of this article is that it does not indicate in detail the feasibility of human rights regime rather calling on general reforms of actions of intelligence agencies.

In relation to governing framework in Africa, this paper looks at works of authors T.S Bulto, Abdulrauf *et al* and Greenleaf. While T.S Bulto discusses the extraterritorial reach of states' human rights duties in the African human rights system, the other two authors discuss the existing cyber security and data protection frameworks in Africa.[20]

T.S Bulto describes how to answer the question 'to whom' and 'on whose' behalf the obligations are to be fulfilled in the African Charter.[21] The author assess the African Charter, related jurisprudence of the African Commission, and relevant international and regional human rights treaties and case law, which may be relied upon as 'inspirational sources' for the interpretation

[16] Milanovic, Supra note 4, p. 141.
[17] OHCHR Report, Supra note 9.
[18] See Digital Rights Ir. Ltd. v. Minister for Commc'n, (Joined Cases C-293/12 & C-594/12, E.C.R. I-238, 2014).
[19] International Covenant on Civil and Political Rights, (adopted Dec. 16, 1966), S. Exec. Rep. 102–23, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976), [hereinafter ICCPR]; Convention for the Protection of Human Rights and Fundamental Freedoms E.T.S. No. 5, (enterd in to force Nov. 4, 1950), [hereinafter ECHR].
[20] T.S Bulto," Patching The 'Legal Black Hole': The Extraterritorial Reach of States' Human Rights Duties in the African Human Rights System", SAJHR, Vol 27, (2011), p. 249 -278; See also, Lukman Adebisi Abdulrauf and Charles Manga Fombad, " The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa? ", Institute for International and Comparative Law in Africa , forth coming article, (2017); See also, Graham Greenleaf and Marie Georges, "The African Union's data privacy Convention: A major step toward global consistency?", Privacy Laws & Business International Report, Vol 131 (2014), p. 18-21.
[21] T.S Bulto, Supra note 20, p. 249.

and application of the African Charter. The shortcomings of this work is that it's not written in the context of establishing a framework for FDS and also does not focus on the 'right to privacy' rather on human rights in general.

The last two authors in this group focus on the detailed explanation of the African Union's cyber security and data protection convention (AUCSDP) [22] as a framework to govern cyber security and data protection in the continent. Abdulrauf and Frombad's article has a more detailed description of existing cyber security and data protection frameworks in the Africa, while the article by Graham Greenleaf and Marie Georges only focuses on describing in detail provisions of the AUCSDP. Although both articles are very informative as to the how Africa is currently dealing with cyber security and data protection, both are not specific to the issue of FDS.

All the above discussed authors offer different approaches to dealing with the issue of FDS governance and extraterritorial privacy protection, this research will use these different approaches in order to identify a viable framework for FDS governance in Africa. This is done by not solely applying a single regional framework (such as the AUCSDP) to the issue, but rather cumulatively utilizing the existing international and regional frameworks of human rights to complement the existing African regional frameworks for human right and data protection.

1.6. Scope and Limitations of the Research

The scope of this study focuses on 'Foreign Digital Surveillance' rather than a wider category of 'surveillance', so the legal assessment does not cover domestic surveillance acts and acts attributable to non-state actors. Specifically, this research takes a look at well documented FDS programs such as PRISM, TEMPORA and other similar program in Africa as a reference point. The legal instruments covered this research are international human rights instruments such as ICCPR, UDHR, ECHR and the African human rights and data protection frameworks. Other supplementary human right frameworks and international law sources such as case law will also be considered. The researcher has chosen to discuss the international and regional human rights instruments in conjunction with African legal frameworks because they are the most widely used, informative and progressive in discussing the right to privacy and FDS.

[22] African Union Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV), (2015), [herein after AUCSDP].

1.7. Research Design and Methodology

This study is descriptive, narrative and analytical. It describes impacts of FDS programs on the right to privacy and it narrates its extraterritorial application in international and regional human rights instruments as a possible remedy. It also analyzes how these instruments can aid the existing African regional framework in dealing with FDS. Extensive desk research has been carried out on existing literature through published and unpublished books, journal articles, official reports, decisions, international legal instruments and scholastic resources. The primary sources are mainly international and African regional human rights instruments such as Universal Declaration of Human Rights (UDHR), African Charter on Human and Peoples' Rights (ACHPR or AU Charter), ICCPR, ECHR, and other instruments such as AUCSDP. While several UN resolutions, conventions, case laws, general comments and various meetings and communiqués have also been important sources. This research will follow a doctrinal based research method. The researcher has chosen this design because he has found it most suitable to achieve the specified objectives of the research. Finally, the reliability and validity of these sources will be strictly considered by the researcher.

1.8. Proposed Chapter Breakdown

This research will have a total of five chapters including an introductory chapter where the proposal of the research will be discussed. Chapter two will first discusses the evolution and current nature of the right to privacy and FDS programs, and then it will highlight the relation between the concepts of right to privacy and FDS establishing a nexus.

Chapter three assesses the extraterritorial application of the right to privacy and FDS. The chapter will then evaluate the criteria's for extraterritorial application of human rights in the case of FDS. To this end, issues such as "legality of interference" and "effective control" in conjunction with recent developments in international human rights law will be analyzed. Chapter four will first detail the existing data and human rights protection frameworks possibly governing FDS in Africa and the possible gaps they may have. It will then debate how extraterritorial application of human rights, specifically the right to privacy can help fill these gaps. The last chapter of this research will include a brief conclusion and recommendation as to dealing with the issue of FDS in the African regional context.

Chapter Two:

FDS and the Right to Privacy

2.1. Introduction

This chapter describes the concept of the right to privacy by answering baseline question of 'who has the right to privacy?' in international human rights law and how this right has been connected to the concept of citizenship. This chapter will also identify a nexus between the concept of FDS and the right to privacy by outlining certain foreign surveillance programs that directly apply to the extraterritorial and transnational nature of surveillance.

2.2. Who has the Right to Privacy in International Human Rights Law?

The 'modern' concept of privacy has its foundations from the social protection of property, personal effects and spaces.[23] In the beginning of the 20th century the idea of an independent concept of privacy developed tying itself closely to the emergence of the industrial age.[24] The actual term 'privacy' has been notoriously difficult to define, and throughout its development it has been termed as a right, a condition, a function, a choice, and, or, a need.[25]

The first two scholars to have defined it as a 'Right' and gave it a novel legal theory were Samuel Warren and Louis Brandeis, placing the right to privacy in a distinct category of an individual's right to be left alone.[26] This instilled the idea that one had the distinct inherent individual rights categorized as 'life, liberty and property' for which the sub category of "life" contained the right to privacy and the right to be left alone.[27] A 'workable' concept of privacy first emerged when Wilborn offered the definition entailed "freedom from unwarranted and

[23] Rolf H. Weber and Dominic N. Staiger, "Bridging the gap between Individual Privacy and Public security", Groningen Journal of International Law, Vol 2, (2015), p. 2.
[24] Dorothy J. Glancy, "The Invention of The Right To Privacy", Arizona Law Review, Vol 1, (1979), p. 21.
[25] J. Michael, "Privacy": in D. Harris and S. Joseph, eds., "The International Covenant on Civil and Political Rights and United Kingdom Law", Oxford Clarendon Press, (1995), p. 333; Noted in Kampmark, Supra note 8.
[26] Glancy, Supra note 24, p. 4.
[27] Samuel D. Warren and Louis D. Brandeis, Harvard Law Review, Vol 4, (Dec. 15, 1890), p. 193-220.

unreasonable intrusions into activities that society recognizes as belonging to the realm of individual autonomy".[28]

Whether one accepts privacy in any of its forms prescribed above, it has since encompassed many facets.[29] These facets are categorized as "Informational Privacy" which involves freedom from unlawful interference with one's personal data. "Bodily Privacy" which concerns the protection of people's physical bodies from invasive procedures and practices. "Privacy of communications" that includes the security and privacy of mail, telephones, email and other communication; and lastly "Territorial Privacy" which concerns setting limits on the intrusion of an individual's home and other property. Most international and regional human rights law instruments include 'the right to privacy' with emphasis added to communications and territorial privacy usually in the wording of a prohibition against interference with one's 'privacy, family, home or correspondence'.[30] The most prominent and the most widely used human rights law instruments such as the universal declaration of human rights (UDHR), ICCRP, ECHR and the American convention on human rights (ACHR) contain this right.[31]

Article 17 of the ICCPR provides that[32]:

> *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honor and reputation…. Everyone has the right to the protection of the law against such interference or attacks."*

---

[28] S. E. Wilborn, "Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace," Georgia Law Review, Vol 32, (1998), p. 825, 833; Noted in Kampmark, Supra note 8.

[29] DeVries, Supra note 7.

[30] The American Convention on Human Rights, Article 11; UN Convention on the Rights of the Child, Article 16; Arab Charter on Human Rights, Article 21. (The African Charter on Human and Peoples' Rights does not include a provision concerning privacy rights, although the African Charter on the Rights and Welfare of the Child does include such a provision at Article 10); See African Charter on the Rights and Welfare of the Child, Art. 2, (opened for signature July 11, 1990), (OAU Doc.CAB/LEG/24.9/49, entered into force Nov. 29, 1999); See also African (Banjul) Charter on Human and Peoples' Rights (adopted 27 June 1981, OAU doc CAB/ LEG/67/3 rev 5, 21 ILM 58, 1982), (entered into force 21 October 1986)

[31] Australia ratified the ICCPR on August 13, 1980; Canada on May 19, 1976; France on November 4, 1980; New Zealand on December 28, 1978; Russia on October 16, 1973; the United Kingdom on May 20, 1976; See ICCPR, Supra note 19. The U.K., France, and Russia are also parties to the European Convention of Human Rights and subject to the compulsory jurisdiction of the European Court of Human Rights; See Council of Europe, Status of Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Eur. Treaty Off., (http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CM=8&DF=08/02/2014&CL=ENG); last visited on June 12, 2016; See also Art 12 Universal Declaration of Human Rights, (G.A. Res. 217 (III) A, U.N. Doc. A/RES/217III), (Dec.10, 1948), [hereinafter UDHR]

[32] ICCPR, Art. 17.

While Article 8 of the ECHR stipulate[33]:

> *"Everyone has the right to respect for his private and family life, his home and his correspondence……There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

.

The American convention on human rights also includes a 'right to privacy'.[34] While many states have not ratified the ACHR most states in the region including the U.S. have ratified the Charter of the Organization of American States and the American Declaration of the Rights and Duties of Man (American Declaration) and had cases before the Inter-American Commission on Human Rights (IACHR) on the basis of the American Declaration.[35] The jurisdictional provision of the ACHR (Article 1) resembles a hybrid of the ICCPR and ECHR provisions, stating in relevant parts that states parties to the "Convention undertake to respect the rights and freedoms recognized herein and to ensure to all persons subject to their jurisdiction … the free and full exercise of those rights and freedoms." The American Declaration does not contain a jurisdictional provision however it has established by the IACHR in the *Donoso v. Panama* case that "a legitimate purpose, must meet the requirements of suitability, necessity, and proportionality which render [them] necessary in a democratic society". Also in *Escher v. Colombia* the IACHR concluded that the right to privacy must be "statutorily enacted".[36] This has even led the court to decide that actions such as, interception of telephone communications without the consent of the callers constitutes an interference with the right to privacy.[37]

---

[33] ECHR, Art. 8.
[34] The Organization of American States (OAS), American Convention on Human Rights, 'Pact of San Jose', Costa Rica, (22 November, 1969), Art. 11.
[35] The fact that the U.S. responds to actions against it before the IACHR suggests that it accepts that the American Declaration binds the country internationally: See Roach v. United States, (Case no 9647), (Resolution No. 3/87, OEA/Ser.L/V/II.71, doc.9 rev.1), (1987), Inter-Am. Comm'n H.R, p. 46-49; See also, e.g., Lenahan (Gonzalez) v. United States, (Case 12.626, Report No. 80/11), (2011), Inter-Am. Comm'n H.R.
[36] See Donoso v. Panama, Judgment, (ser. C, No. 193), (Jan. 27, 2009), Inter-Am. Ct. H. R, p.56; See also Escher v. Colombia, (ser. C, No. 200), (July 6, 2009), Inter-Am. Ct. H. R., (Judgment), p. 130.
[37] Ibid.

Privacy in Africa is described by scholars as being "foreign because of its communal orientation as against individualism which is perceived to be a western idea".[38] This is supported by the African Charter on Human and Peoples' Rights not containing a 'right to privacy'. It simply states that "everyone has the right to have his honor respected and his dignity recognized… No one may be the subject of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation…everyone has the right to protection of the law against such interference or attacks".[39]

To better understand the 'right to privacy' and how it can be relatable to the concepts of FDS the next part of this chapter will discuss how privacy is shaped by its historical ties to citizenship and how it has evolved to a more universal concept forming a nexus with FDS.

2.3. Citizenship, Privacy and FDS

A look at the history of most states suggests that there is a noticeable distinction towards privacy rights granted to citizens and non-citizens, surveillance conducted on citizens and that conducted on foreigner as well as surveillance conducted on national soil and outside states territory.[40] The justifications granted for this citizen oriented approach as per Olin Kerr stems from the perception that "governments have legitimacy because of the consent of its citizens and those in its borders" and therefore must favor them.[41] However the construct of human rights runs contrary to this, as put eloquently by Ronald Dworkin, "the domain of human rights has no place for passports."[42] This has led to scholars like Margot Salomon to help develop the concept of 'the spatial reach of human rights' driven mainly by the need to regulate transnational and

[38] AB Makulilo, "Myth and reality of harmonisation of data privacy policies in Africa", Computer Law & Security Review , Vol 31 (2015), p. 82.

[39] Notably, Article 62 of the ACHPR requires States to submit periodic reports detailing the legislative and other measures that they have adopted to give effect to the rights guaranteed by the Charter including the right to privacy while sub-regional entities such as the Economic Community of West African States (ECOWAS) have created agreements that contribute to the protection of the right to privacy, such as a supplementary act on the protection of personal data in 2010, and a directive on fighting cyber-crime within the community in 2011.

[40] For example Australia, New Zealand and Canada have investigative and national defense acts which defines persons a being citizens or having permanent residence.

[41] Orin Kerr, "A Reply to David Cole on Rights of Foreigners Abroad", Lawfare, (Nov. 2, 2013), (www.lawfareblog.com/2013/11/a-reply-to-david-cole-on-rights-of-foreigners-abroad/); last visited on June 12, 2016.

[42] Ronald Dworkin, "Is Democracy Possible Here?"; as Noted in Milanovic, Supra note 4, p. 98.

extraterritorial actions of states.[43] Naturally, a question of whether individual (other than citizens) enjoy the right to privacy in regard to a particular state is asked. An answer is to be had on whether privacy rights enshrined in international and regional human rights treaties can be applied extraterritorially and the concept that citizen's privacy rights 'must not be treated preferentially' in relation to foreign nationals.[44] This concept of human rights having extraterritorial reach, represent a 'revolutionary' advance on how the right to privacy as a human rights is viewed.[45]

2.3.1. The Nexus: Foreign Surveillance Programs and the Right to Privacy

The most prominent 'surveillance capable' states use a variety of methods to gather intelligence having vast implication on the enjoyment of the right to privacy. Documented FDS programs used by the NSA include demand of "metadata" and "content data" from telecom providers, having direct access to the servers of internet giants such as Google, Facebook, and Apple, interception of huge fiber-optic communications cables; implant of software in devices such as phones and computers either by intercepting packages or remote installation for remote access to the devices' data; quantification and later tracking of the user based solely on an IP-address or a phone number and the record of specific transactional data such as the time and date of a call.[46]

This means that intelligence agencies no longer need to be physically located near the source of their preferred information.[47] Specifically, the 'PRISM' program is of a special value to the NSA intelligence activities, because it grants direct access to the servers of the private companies and enables the collecting of data including search history, email content, the transfer of files and live chats. [48] Disclosures have also been made about the 'TEMPORA' program used by the GCHQ. This involves the placement of data interceptors by the GCHQ on international fibre-optic cables

[43] ME Salomon, "Global Responsibility for Human Rights: World Poverty and the Development of International Law", (2007); as discussed in T.S Bulto, Supra note 20, p. 249.
[44] Marko Milanovic, "Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy", Oxford University Press, (2011), p. 67–83
[45] See T.S Bulto, Supra note 20, p. 249.
[46] See Davenport, Supra note 6; See also, Greenwald & MacAskill, Supra note 6.
[47] Khalil, Supra note 8, p. 925.
[48] Greenwald & MacAskill, Supra note 6.

conveying internet data within and out of the UK, these cables include transatlantic connections between the US and Europe.[49]

The European Parliament has even adopted a resolution on the surveillance programs expressing concern over such advancements, explicitly on how these programs affect Europeans' fundamental rights and freedoms (such as privacy).[50] A former UN-rapporteur on the protection of human rights while countering terrorism also stated this limitation upon the right to privacy by the surveillance architecture of the NSA and GCHQ violates the legal obligations of the U.S. under the ICCPR.[51]

Also in Africa there are documented actions of Nigerian government developing a comprehensive electronic ID card scheme with the assistance of an American company, MasterCard where there could be vast movement of personal information from Nigeria to the United States where the headquarters of MasterCard is situated. [52] There have also been allegations made towards African governments having also participated in mass surveillance alongside the United States of America, with several states cited as having procured mass surveillance technologies by popular German producer Trovicor.[53] Zimbabwe has also been implicated as having exceptionally broad mechanism for surveillance allowing oversight of civilian and foreign communications. [54] This assertion was made through the government purchase of Portnet Software (a 51% information communication services provider to the country) through Zarnet (a wholly government-owned entity).[55]

---

[49] 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); last visited on June 12, 2016.

[50] Statement made by Professor Martin Scheinin, LIBE Committee Inquiry, on Electronic Mass Surveillance of EU Citizens, as discussed in; Joergensen, R., "Can human rights law bend mass surveillance?", Internet Policy Review, Vol 3(1), (DOI: 10.14763/2014.1.249), (2014), (http://policyreview.info/articles/analysis/can-human-rights-law-bend-mass-surveillance); last visited on June 12, 2016.

[51] Ibid.

[52] See, J Oguntimehin, "Implications of Nigeria's National ID card", (http://www.iafrikan.com/2014/09/30/nigeria-national-id-card/#sthash.aDBRkrnA.dpuf); last visited on June 12, 2016.

[53] "Spy Tech Companies & Their Authoritarian Customers, Part II: Trovicor and Area SpA", Electronic Frontier Foundation, (2012), (https://www.eff.org/deeplinks/2012/02/spy-tech-companies-their-authoritarian-customers-part-ii-trovicor-and-area-spa); last visited on December 27, 2016.

[54] See Discussions in Gabriella Razzan, "Human Rights and Information in Africa: A reflection on trends by 2016", Published by fesmedia Africa, Friedrich-Ebert-Stiftung, (2016).

[55] Ibid.

2.4. Conclusion

The evolution of the concept of privacy and sophistication of communication surveillance has created a nexus between how we can regulate state surveillance and how to guarantee the right to privacy of individuals. While privacy in the past was tied to the issue of citizenship, the developments in the extraterritorial application of human rights and documented FDS capabilities of states have changed this dynamic. This chapter has further outlined the fact that foreign surveillance programs do impact the right to privacy by discussing different sophisticated surveillance programs. This is also true in Africa, where FDS actions of states could have implications on enjoyment of privacy rights of Africans.

Chapter Three:

Extraterritorial Application of the Right to Privacy and FDS

3.1. Introduction

After establishing a nexus between rights to privacy and FDS in the previous chapter, the following chapter will discuss in detail the extraterritorial application of the right to privacy in international human rights. It will start by describing three models[56] and approaches to extraterritorial application in international human rights law. Assessments will also be made as to whether the criteria's for extraterritorial application in international human rights law (such as 'effective control' and 'legality of interference') can be functional to the FDS context. In depth analysis will also be made on the current jurisprudence towards extraterritorial application of international human rights treaties with special focus on the ICCPR, ECHR and other recent developments.

3.2. Models Extra Territorial Application

A) The Spatial Model

One of the first articulations of the spatial model of extraterritorial application was made by the European court on human rights (ECtHR) in the *Loizidou* case and the UN Human Rights

[56] As discussed in Milanovic, Supra note 4, p. 113 – 120.

Council (HRC) in the case involving the legal consequences of the construction of the wall in occupied Palestine territory.[57] This model stipulates that jurisdiction is described as having *de facto* effective control over an area. The Spatial model of jurisdiction appeals to the fact that a state has 'effective control' over a territory so it is only right that it grants human rights or has human rights obligation toward those who inhabit this territory.[58] In addition, the European Court on human rights also held that what matters is the *fact* of such control, regardless of whether it was obtained lawfully or unlawfully.[59]

However, the HRC has also stated that "a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State party, even if not situated within the territory of that State party".[60] Decisions from the ECtHR and the IACHR have confirmed this extraterritorial application of human rights and established the test of "effective control" [61] and "authority and control"[62] (these principles will be discussed below).

While the spatial model dose have a clear outline, giving protection to those who occupy its territory, this model also has drawbacks when applied to human rights protection in times of FDS. These drawbacks can be exemplified by the fact that a state can violate human rights without control over and area (like actions of state use of targeted drone strikes killings and foreign black sites for interrogation).[63] This makes "control" entirely irrelevant to the substance of the violation; thus the more unsatisfactory and unappealing the spatial model becomes to FDS.[64] To deal with this problem shrinking of the size of the area has also been applied in some

[57] See Loizidou v. Turkey, (App. No. 15318/89, 310, Sec. A, 1995), ECtHR., (Judgment), Para. 62.; See also Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, (Advisory Opinion 136, 179 on July 9, 2004), I.C.J; See also Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), (Judgment), (Dec. 19, 2005), I.C.J.; For a detailed explanation of the Spatial model See Ralph Wilde, "Triggering State Obligations Extraterritorially: The Spatial Test in Certain Human Rights Treaties", Israel Law Review, Vol 40, (2007), p. 503; See also discussions in M Gondek, "Extraterritorial Application of the European Convention on Human Rights: Territorial Focus in the Age of Globalisation?", Netherlands International Law Review, Vol 52, (2005), p. 349, 351.

[58] SI Skogly, "Extraterritoriality: Universal Human Rights without Universal Obligations?"; in S Joseph & A McBeth (eds) Research Handbook on International Human Rights Law (2010).

[59] Loizidou Case, Supra note 57.

[60] U.N. Human Rights Comm., General Comment No. 31: Nature of the General Legal Obligation on States Parties to the Covenant, (U.N. Doc. CCPR/C/21/Rev.1/Add.13), (2004), [herein after GC31].

[61] Ibid.

[62] See Alexandre v. Cuba, (Case 11.589, Report No. 109/99, 1999), Inter-Am. Comm'n H.R., p. 23

[63] Cases are currently pending before the European Court against Poland for allowing or failing to prevent the human rights abuses in the "black sites." See, e.g., Al Nashiri v. Poland, (App. No. 2876/11, 2014), ECtHR. (Judgment); Husayn (Abu Zubaydah) v. Poland, (App. No. 7511/13, 2014), ECtHR. (Judgment).

[64] Milanovic, Supra note 4, p. 113.

cases[65] but the more one shrinks the size of the area, the more it is likely to collapse into a concept of jurisdiction as control over individuals, rather than spaces.[66]

B) The Personal Model

This model first formulated by the European Commission on human rights is framed on the basis that jurisdiction of human rights treaties *vis a vis* states is derived from the 'authority and control' exercised by states over 'individuals'.[67] A more detailed understanding of this model was also realized by the HRC's case between *Lopez and Uruguay,* in which the committee established the personal model on the basis of 'universality of human rights". [68] The HRC also reiterated the concept of 'universality of human rights' in General Comment No. 31 (GC31).[69] The first drawback of this model is impossibility in limiting its application, leading to the perception of human rights treaties governing every extraterritorial action of states. This led the ECtHR to render a decision in the *Bankovic case,* stating that a North Atlantic Treaty Organization (NATO) airstrike in Kosovo did not put the victims of the airstrikes under the jurisdiction of the NATO states since there were "no ground troops" to establish "effective control" over an area thus ignoring principles of the personal model.[70] Understandably criticisms mounted on this judgment leading the ECtHR to reset its path on the question of extraterritorial application in the *Al-Skeini case*.[71] In this case the court reaffirmed the validity of both the spatial model and the personal model regarding state agent authority.[72] This gave the impression

[65] There have been a number of cases applying the spatial model to ever decreasing areas such as a military prisons, ships and aircrafts. See Al-Saadoon v. United Kingdom, (App. No. 61498/08, 2010) ECtHR. (Judgment); See also Jamaa v. Italy, (App. No. 27765/09, 2012), ECtHR. (Judgment); See also Medvedyev v. France, (App. No. 3394/03, 2010) ECtHR. (Judgment); See also Ocalan v. Turkey, (App. No. 46221/99, 2005-IV), ECtHR. (Judgment).
[66] See Wilde, Supra note 57, p. 503.
[67] Cyprus v. Turkey, (App. Nos. 6780/74 & 6950/75, 2,1975), Eur. Comm'n H.R., (Dec. & Rep.), Para. 8.
[68] Lopez v. Uruguay, (Comm. No. R.12/52, U.N. Doc. Supp. No. 40 A/36/40, 1981). U.N. Human Rights Comm., Paras. 12.1–12.3, p. 176.
[69] See GC31, Supra note 60, See; See also Loizidou, supra note 57; See also Alexandre, Supra note 62; See also Issa And Others v. Turkey, (2004), ECtHR.
[70] Bankovi´c v. Belgium (Decision), (App. No. 52207/99, 2001-XII), ECtHR.
[71] See Olivier De Schutter, "Globalization and Jurisdiction: Lessons from the European Convention on Human Rights", Baltic Y.B. Intnternatioanl Law, Vol 6, (2006), p. 183; See also Alexander Orakhelashvili, "Restrictive Interpretation of Human Rights Treaties in the Recent Jurisprudence of the European Court of Human Rights", European Journal of International Law, Vol 14, (2003) p. 529; See also Erik Roxstrom, Mark Gibney & Terje Einarsen, "The NATO Bombing Case (Bankovi´c et al. v. Belgium et al.) and the Limits of Western Human Rights Protection", B.U. Intternatial Law Journal, Vol, 23, (2005), p. 55; See generally Al-Skeini v. United Kingdom, (App. No. 55721/07, 2011) ECtHR., (Judgment).
[72] Id, Al-Skeini v. United Kingdom, Paras. 138–40.

that the court was tailoring and dividing the convention rights in comparison to the approach taken in *Bankovic*.[73]

C) State Obligations Model

This more recent model [74] bases jurisdiction on the distinction between the overarching positive obligation of states to "secure" extending to preventing human rights violations by third parties; and the negative obligation of states to "respect", which only requires states to refrain from interfering with the rights of individuals without sufficient justification.[75] Meaning "jurisdiction" could only primarily imply "effective overall control over areas" while the overarching positive obligation would be "predicated on a state having such control over an area" because "in the overwhelming majority of situations the state actually needs such control in order to be able to comply with this obligation".[76] The negative obligations are described as 'respect' for human rights "territorially unlimited and not subject to any jurisdictional threshold". This coincides with international human rights instruments such as the UDHR and ICCPR which have 'universal connotations' with an obligation of "ensure" attached to it.[77]

After looking at these three models, the next part of this chapter will discuss existing approaches to extraterritorial application of human rights.

3.3. Approaches to Extraterritorial Application of Human Rights Treaties

One of the primary sources of the right to privacy in international law is the ICCPR. Article 2(1) of this instrument imposes a duty upon states "to respect and to ensure to all individuals within its territory *and* subject to its jurisdiction the rights recognized in the present Covenant."[78] The

[73] Milanovic Explains that what occurred recently in Libya, The use of drones in areas not under a state's control would likewise be outside the scope of the Convention per Al-Skeini and Bankovi´c in which the UK considers the Al Skeini judgment to be set in the factual circumstances of UK's past operations in Iraq and having no implications for its current operations elsewhere; See, Milanovic, Supra note 4, p. 118.
[74] M.Craven "The Violence of Dispossession: Extra- Territoriality and Economic, Social and Cultural Rights'; in MA Baderin & R McCorquodale (eds), Economic, Social and Cultural Rights in Action, (2007); See also Milanovic, Supra note 4, p. 120; See also Beth Van Schaack, "The United States Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change", International Law Studies, Vol 90, (2014).
[75] See Rona & Aarons, " State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cybrrspace", J. Nat'l Security L. &Pol'y , Vol 8, (2016), p. 1; See also ME Salomon, Supra note 43.
[76] Ibid,
[77] Van Schaack, Supra note 74.
[78] ICCPR, Art 2.

term 'and' in this article has led to debates as to whether the ICCPR applies extraterritorially. [79] Understanding this debate is important to determine the extraterritorial application of human rights to issues of FDS. So the following will discuss the different approaches taken to interpret this article.

A) The US Approach

As of 2014, the US position on ICCPR was that it does "not" and "has never" applied extraterritorially. [80] This stand was substantiated by the U.S. notion that the Vienna Convention on the Law of Treaties (VCLT) requires reading a treaty 'in accordance with the ordinary meaning . . . of its terms.' so that "ordinary" meaning of two conditions connected by the conjunctive, "and" is an obligation arising only upon the satisfaction of both conditions.[81] This would entail that a state incurs obligations under the ICCPR only to individuals who are both "within its territory" and "subject to its jurisdiction".[82]

However this reading of the ICCPR had its opponents, the most prominent of whom was Buergenthal stating such reading would clash with at least two of the ICCPR's provisions.[83] This refereed to the 'lack of meaning' of those provisions such as the right of the nationals of a state "to return to that state" and "the right not to be tried in absentia" if they do not protect individuals at least temporarily outside of a state's territory. [84]

In 2012, before the US delegation was to present its 4th periodic report to the human rights committee, two internal memoranda written by Harold Koh (then the legal adviser to the State

---

[79] Peter Margulies, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism", Fordham Law Review, Vol 82, (2014), p. 2137.

[80] The United States previously reiterated that 'the obligations assumed by a State Party to the International Covenant on Civil and Political Rights applied only within the territory of the State Party'; See Georgieva, Supra note 3, p. 108.

[81] Article 31 and 33 of the VCLT contains three approaches to treaty interpretation in which the first approach centers on the actual text of the provision in question. 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. Additionally, the VCLT requires reading of the Covenant in good faith and consistent with its ordinary meaning. According to Georgieva, the US position seems to be the most natural one, considering the literal meaning of 'and' as a conjunction between 'within its territory' and 'subject to its jurisdiction'; See Vienna Convention on the Law of Treaties, (1155 UNTS 331, 8 ILM 679), (adopted 23 May, 1969, entered into force 27 January 1980), Art 31 (1); See also Georgieva, Supra note 2, p. 109.

[82] Robert J. Delahunty & John C. Yoo, "What Is the Role of International Human Rights Law in the War on Terror?", Depaul Law Review, Vol 59, (2010), p. 803, 835.

[83] Thomas Buergenthal, To Respect and To Ensure: State Obligations and Permissible Derogations; In the International Bill of Rights (Louis Henkin ed., 1981), p. 72, 74.

[84] Id., Discussions by Buergenthal in reference to Art 12(2), (4) and Art 14(3) (d) of the ICCPR.

Department) were published by the New York Times.[85] The first of these memos discussed extraterritorial application of the ICCPR.[86] This memo states the U.S. categorical opposition to the extraterritorial application of the ICCPR was "fundamentally flawed and should be abandoned".[87] It further indicated the language of the ICCPR is 'not clear' and 'open to several possible interpretations', while reading it to categorically disallow extraterritorial application would be contrary to the treaty's object and purpose.[88] However, Koh's opinion did not persuade the Obama administration given it would call for significant alterations to existing polices especially in regards to extraterritorial targeting or detention of suspected terrorists.[89]

Consequently, the U.S. did not change its position leading to the HRC's to express its disappointment.[90] This disappointment stemmed the fact that in *Lopez v. Uruguay* the HRC had stated Uruguay violated its obligations under the Covenant when its security forces abducted and tortured a Uruguayan citizen then living in Argentina. Stating that it would be 'unconscionable' to interpret the ICCPR towards permitting a State party to violate of 'the Covenant on the territory of another State', for violations it could not perpetrate on 'its own territory'."[91] Subsequently in General Comment 31, the HRC asserted that the ICCPR rights applies to 'anyone' within the 'power or effective control of State Party', even if not situated within the territory of the State and that "enjoyment of Covenant rights is available to all individuals, may find themselves in the territory or subject to the jurisdiction of the State Party" regardless of nationality or statelessness.[92] The HRC also confirmed this position to the Israeli government's assertion that the ICCPR did not apply to its conduct in the occupied territories.[93]

---

[85] See Charlie Savage, "U.S. Seems Unlikely to Accept That Rights Treaty Applies to Its Actions Abroad", N.Y. Times, (Mar. 7, 2014), p. A6.

[86] U.S. Dep't of State, Office of the Legal Advisor, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights (Oct. 19, 2010), (http://justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf.); last visited on June 12, 2016; See also U.S. Dep't of State, Office of the Legal Advisor, Memorandum Opinion on the Geographic Scope of Application of the Convention Against Torture and Its Application in Situations of Armed Conflict (Jan. 21, 2013), (http://justsecurity.org/wp-content/up loads/2014/03/state-department-cat-memo.pdf.); last visited on June 12, 2016. [hereinafter Koh's Opinion].

[87] Id., p. 7 and 8.

[88] See explanation in Milanovic Supra note 4.

[89] Savage, Supra note 85.

[90] Ibid.

[91] Lopez v. Uruguay, Supra note 68.

[92] GC 31 Supra note, p. 60.

[93] Legal Consequences of the Construction of a Wall, Supra note 57.

Conversely there are arguments made suggesting that the HRC 'Interpretations' or 'Comments' are not binding and also that the ICCPR does not bind the U.S. in 'domestic law' to protect 'the right to privacy of citizens and aliens alike.'[94] Additionally, no one can obtain a legal remedy in U.S. courts for U.S. violations of the ICCPR given federal courts 'are not bound to enforce its terms'.[95] Nevertheless, the Obama admission has moved to clarify the U.S. stand, by acknowledging the 'legitimate privacy interests' of both U.S. and non-U.S. persons, while affirming the U.S. commitment to core principles of the ICCPR.[96] Leading to a narrowing the definition of foreign intelligence information,[97] while asserting that U.S. bulk collection programs would be only used for justifiable national security treats.[98]

B) The Protective (Sweeping) Approach

This approach to extraterritorial application is on the basis of the First Optional Protocol the ICCPR, in which the HRC shall hear individual complaints against state parties to the ICCPR.[99] The HRC indicated that states are always bound, within their territory and in other areas subject to their jurisdiction, to both respect and ensure that individuals receive rights under the ICCPR.[100] Scholars like Buergenthal believe this approach "would be to merely import ones policy preferences without regard to the text" additionally putting the predictability, legitimacy, and connection to state consent in danger.[101] With this formulation it would be difficult for a state to 'spot its open ended obligations' under the HRC's expansive rule. [102]

---

[94] Daniel Severson, "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change", Harvard International Law Journal , Vol 56, (2015), p. 1.

[95] Severson argues that the Supreme Court has held that only self-executing treaties provide rules of decision for U.S. courts and so when the Senate provided its advice and consent to the ICCPR, it attached a declaration that Articles 1–27 of the treaty are not self-executing; Id, p. 99.

[96] See Press Release, The White House, Office of the Press Sec'y, Presidential Policy Directive/PPD-28, (Jan. 17, 2014), p. 5; See also Benjamin Wittes, " The President's Speech and PPD-28: A Guide for the Perplexed", Lawfare (Jan. 20, 2014, 11:02 AM), (http://www.lawfareblog.com/2014/01/the-presidents speech-and-ppd-28-a-guide-for-the perplexed/#.Ut23FKMo6po.); last visited on June 12, 2016.

[97] Exec. Order No. 12,333, 3 C.F.R. 200, 204–05 (1981), amended by Exec. Order No. 13,470, 3 C.F.R. 218, 227 (2008), (reprinted as amended), 50 U.S.C.401 app. (Supp. V 2011), p. 934–43.

[98] Ibid.

[99] Optional Protocol to the International Covenant on Civil and Political Rights, Art. 1, opened for signature Dec. 19, 1966, (999 U.N.T.S. 302), (entered into force Mar. 23, 1976). Although not ratified by the U.S the optional protocol shows actions of the international community to support the disjunctive reading.

[100] Ibid.

[101] Buergenthal, Supra note 83.

[102] Oona A. Hathaway, "Do Human Rights Treaties Make a Difference?", Yale Law Journal, Vol 111, (2002).

C) The Middle Ground

An alternate approach is seen in the jurisprudence of the ECHR interpreting ICCPR applicability with due regard to its "protective purpose" and the on the 'nature of duties' it imposes on states requiring *de facto* jurisdiction (i.e. control over territory or persons).[103] The ECtHR explained that the test of jurisdiction could be met either through the spatial and personal model when a state's agents 'exercise control and authority over an individual' or in alternate 'exercises effective control over a geographic area, either directly, through its own armed forces, or through a subordinate local administration.'[104] Meaning a state may have jurisdiction over an individual without occupying a whole territory.

Additionally in of *Ocalan v. Turkey* a case involving the handing over of suspect to turkey in Kenyan territory,[105] the aforementioned suspect was considered by the ECtHR to be a within the 'jurisdiction' of Turkey after a handover took place in Kenyan territory 'by the mere fact that turkey officials had exercised some public powers over the suspect'.[106]

3.4. The Possible Issues in Extraterritorial Application of the Right to Privacy in the Case of FDS

Chapter three has briefly highlighted the different models and approaches extraterritorial application of international human rights treaties. Hence, the next chapter will take an indebt look at criteria's that need to be fulfilled for extraterritorial application the right to privacy in cases of FDS.

Recent developments in international human rights law will also be assessed in this context. This discussion is relevant to the African context as it is gives insightful lessons (i.e. the extraterritorial application human rights in governing FDS) which could be carried over as lessons to an African regional framework governing FDS.

[103] Margulies, Supra note 79, p. 2148.
[104] Al-Skeini, Supra note 71.
[105] Ocalan v. Turkey, (2005-IV), ECtHR..
[106] See Sarah H.Cleveland, "Embedded International Law and the Constitution Abroad", Colombia Law Review, Vol 110, (2010), p. 225, 232–62.

3.4.1. Criteria's for Application in the HRC and European Regional System

A) Criteria of Effective Control in the Foreign Digital Surveillance Context

One of the key criteria's that should be addressed in the foreign surveillance context is the criteria of 'effective control.'[107] The HRC, in this regard, has a lower degree of practice in the matter of extraterritoriality given it receives 'fewer complaints than its European counterpart the ECtHR'.[108]

Nonetheless, in Judgments like *Lopez v. Uraguay* the HRC has found that States parties are responsible for infringements committed by their foreign diplomatic representative.[109] Also accepting 'extraterritorial application in cases where state agents exercised authority and control over individuals, rather than over areas' as per the *Cyprus case*.[110]

In General Comment 31 the HRC has also stated that a State Party must provide for the Covenant's rights to anyone within its "power" or "effective control", even if that person is not within its respective national borders and regardless of the circumstance in which such power or effective control was obtained.[111] This points toward the maximum protections of human right as some might suggest while other state that this interpretation is a bit "purposive".[112]

But in the context of FDS the actual 'physical control' over persons is not a requirement. Scholars offer different solutions to this problem, the first of which comes from Margulies.[113] He proposes applying a varied version of the 'effective control test' appropriately named the 'Virtual Control Test' with two distinct criteria's. Firstly, it must work closely with the established principles of jurisdiction and secondly it must consider problems in dealing with the modern surveillance capabilities of states.

[107] Milanovic, Supra note 4, p. 81-82.
[108] Georgieva, Supra note 2, p. 111.
[109] Lopez v. Uruguay, Supra note 68.
[110] 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), p. 73.
[111] GC 31, Supra note 60.
[112] Discussion made in Margulies, Supra note 79, p. 2148 – 2150.
[113] Id, p. 2150.

Another approach is forwarded by scholars such as Milanovic, Fidler, and Rona *et al*.[114] This approach suggests that states need to look no further than human rights conventions and norms emphasizing on the 'tripartite typology' of 'respect, protect and fulfill'[115] Categorizing 'the duty to respect as negative obligations and the other two as positive obligations'.[116] The problem with this formulation is that most actions of FDS occur within days or hours giving little time for the foreign state acting abroad to positively ensure or protect human rights, granted it lack the respective powers to adopt any legislative, judicial or administrative or other appropriate measures in order to fulfill its positive legal obligations; so can only make sure to respect and not to interfere with the rights of the individuals.[117]A similar approach taken by Van Schaack suggests that the duty to ensure should be limited to where the individual is both within a state's territory and subject to its jurisdiction.[118] Since states control of their organs and agents they are capable of complying with their negative obligations.[119]

3.4.2. Criteria for Legality of Interference

Article 8 (2) of the ECHR grants a 'public authority' the right to 'interfere' so long as its actions are 'in accordance with the law', 'necessary in a democratic society' and pursue 'legitimate aims'.[120] These 'legitimate aims' are crime and disorder prevention and protection of the rights of others.[121] Article 17 of the ICCPR also cites that 'no one should be subjected to arbitrary or unlawful interference'.[122]

A look at the jurisprudence of both HRC and ECtHR dose suggest similar assessments in this criterion[123] and can be summarized in to three; the first being whether the interference is in

[114] See David P. Fidler, "Cyberspace and Human Rights", in Nicholas Tsagourias & Russell Buchan (eds) Research Handbook on International Law and Cyberspace, (2015); See also Rona and Aarons, Supra note 75.
[115]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); See also Deeks, Supra note 3.
[116] Ibid.
[117] See Rona and Aarons, Supra note 75.
[118] Ibid.
[119] Van Schaack, Supra note 74.
[120] ECHR, Art. 8(2).
[121] Ibid.
[122] ICCPR, Art 17.
[123] See 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),

'accordance with the law'; second being the fulfillment of the 'legitimate aim' criteria; and lastly 'proportionality' in cases where a legitimate aim is fulfilled.[124]

In the first criteria both article 8 (2) of the ECHR and article 17 of the ICCPR require an authorization under national law to interfere with privacy interests on the basis of a generally accessible provisions of law proclaimed prior to interference. The HRC also takes this view.[125] In the *Malone case* the ECtHR had also established a further requirement of accessibility, foreseeability and compatibility with the rule of law, meaning that in 'surveillance cases' a breach of these requirements on the domestic level automatically leads to violations of international human rights provisions.[126] The HRC has acknowledged this stand.[127] An Accessibility requirement also dictates that a person must be given the opportunity to familiarize themselves with the relevant rules and security concerns before surveillance is conducted.[128] When relating this to FDS actions like "PRISM", the U.S. violated this principle when it relied on the FISA Amendments Act of 2008, for 'premeditated targeting' of communications from foreign nationals believed to be not on U.S. soil.[129]

Nardell describes foreseeability as 'when a citizen finds the answer to the question Why me?'[130] This does not mean that individuals have the ability to anticipate when authorities are likely to adopt surveillance measures targeting them so that they can behave accordingly.[131] Rather it relates to compatibility with existing law and judicial supervision of approved surveillance measures.[132]

---

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)

[124] See Georgieva. Supra note 2, p 118.

[125] The HRC has indicated that the interference can be justifiable only in the cases actually envisaged by law and on the part of the ECHR this approach was first articulated in the case of Klaas and Others v Germany, one of the first surveillance cases of the ECtHR; See Klass and Others, Supra note 123.

[126] See Milanovic Supra note 4, p. 68.

[127] Manfred Nowak, U.N. Covenant on Civil and Political Rights: ICCPR Commentary, (Engel 2005) Art 2, p. 401,402.

[128] See Georgiva, Supra note 2, p. 118; See also Liberty vs Other, Supra note 123.

[129] The FISA Amendments Act of 2008, H.R. 6304, 110th Cong. (2008), (https://www.govtrack.us/congress/bills/110/hr6304/text) last visited June 12, 2016; See also discussions by Greenwald and McAskill, Supra note 6.

[130] 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), p. 46.

[131] Ibid.

[132] In Ekimdziev case the Court found that the Bulgarian law did not provide any independent means of review of the intelligence agency's activities; See Ekimdziev v Bulgaria App no 62540/00, ECtHR, (28 June 2007);

The second criterion of 'legitimate aim' is invoked in cases of 'national security', 'the prevention of disorder or crime' or 'prevention of a breach of the peace'.[133] This 'aim' is satisfied with in the auspice of 'necessity', which the ECtHR propose two cumulative approaches of proportionality paying attention to 'the nature, scope and duration of the measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them and the kind of remedy provided by the national law'.[134] The proportionality element when applied to FDS programs dose give states a broad 'margin of appreciation' in cases of serious national threats.[135] In the *Weber case* the ECtHR stated that 'personal data collected for one specific purpose can only be used for another specific purpose if the data could have been independently collected for that purpose'.[136] However establishing legitimate aim could prove problematic for surveillance operations regarding duration of the surveillance, in which under TEMPORA, boundless Informant and PRISM; programs effectively collect data on an on-going basis.[137]

3.5. Recent Developments in International Law Impacting FDS

3.5.1. The OHCHR Reports

One of the most important recent developments in regard to FDS has been the 2014 OHCHR Report. Article 17 of the ICCPR is interpreted in the report, in which interferences of privacy can only be justified if they are not arbitrary and unlawful adopting the framework of legality, necessity, proportionality and other principles established by the International Principles on the Application of Human Rights to Communications Surveillance (IPAHRC). [138]

---

[133] Legitimate aim is rarely challenged by the HRC, case law suggests that states more often than not have convinced the HRC of legitimate aim. However, the ECtHR has established that employing secret surveillance requires adequate and effective safeguards against abuse; See Leander v Sweden. (App no 9248/81), ECtHR, (26 March 1987)

[134] See Weber v. Germany, Supra note 123.
[135] Georgieva, Supra note 2, p. 123-125.
[136] See Weber v. Germany, Supra note 123.
[137] See discussions by Georgieva, Supra note 2, p. 123-127.
[138] The IPAHRC are a set of principles endorsed by over 200 NGO's. These principle include necessity and proportionality with additional safeguards such as giving limited and targeted access to intelligence agencies, not authorizing bulk access to data, insuring that data collected of national security is not used for other propose, specifying data retention parameters such duration, the incorporation of privacy-protective technologies and criminalization of illegal surveillance; See International Principles on the Application of Human Rights to Communications Surveillance, (Herein after IPAHRCS), 10 July 2013, (https://en.necessaryandproportionate.org/text); last visited June 12, 2016.

The report also discusses third party data retention in context of national security as a legitimate interest stating that degree of interference must be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields, with appropriate safeguards like accessibility of domestic legal framework. [139]

Regarding extraterritoriality the report takes an expansive approach stating that human rights obligations of states are triggered when digital surveillance takes place.[140] This relates to having 'effective control' or exercises power over digital communication infrastructure (like tapping of data cables) and exercises of regulatory jurisdiction over a third party controlling such data. It goes on to say that private companies that have been incorporated in a state may be "subject to its jurisdiction" in cases of "data sharing" giving protection to individuals whose privacy right is being infringed (like the instances described in chapter 2, on transfer of data by Nigerian government to foreign company Mastercard).[141] The report in the matter of extraterritoriality tries to focus on the issue of jurisdiction rather than lawfulness of the action, acknowledging the existing gap in regards to those types of surveillance that require no control over the infrastructure at all.

More recently pursuant of resolution 28/16, the now Special Rapporteur on the right to privacy (SRP), Joseph A. Cannataci submitted his own report. [142] This report describes privacy in 2016 as being relevant to a digital age where the internet operates without borders.[143] It describes privacy as an enabling right as opposed an end in itself, 'enabling' the fundamental right to the free, unhindered development of one's personality.[144] On the front of national security and intelligence agencies the SRP stress on the adequacy of oversight mechanisms, the distinction between targeted surveillance and mass surveillance, the proportionality of such measures in a democratic society. Importantly, the SRP has reaffirmed that article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights constitute the basis of the right to privacy in international human rights law.[145]

[139] OHCHR Report, Supra note 9, Para. 20.
[140] Ibid.
[141] Oguntimehin, Supra note 52.
[142] Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, U.N. Doc. A/HRC/31/64, (March 2016), [hereinafter SRP Report].
[143] Ibid.
[144] Ibid.
[145] Ibid.

3.5.2. Recent Case Law

One of the most recent ground breaking cases in regards to the issue of FDS is *Digital Rights Ireland*. [146] It highlights problems faced when private companies retain 'metadata' and how governments can use them as avenues to engage in surveillance acts. This case involves a complaint lodged against the EU Data Retention Directive as violating fundamental principles of privacy and data protection. The European Union Court of Justice (ECJ) examined the compatibility of the directive with the charter stating that it required the collection and storage of metadata produced in electronic communications taken as a whole, allowing conclusions to be drawn concerning the private lives of the persons whose data has been retained.[147] It also did not permit 'the retention of the content of the communication having an effect the freedom of expression guaranteed by Article 11 of the Charter'.[148] Specific to violations on the rights to privacy and data protection by the ECJ assessed whether the Data Retention Directive constituted an interference with Articles 7 and 8 of the EU Charter of Fundamental Rights and if such interference was justified.

The ECJ stated that Articles 3 and 6 of the Directive to retain the metadata had constituted 'in itself an interference with the rights guaranteed by Article 7 of the Charter and if national authorities could access this data it would be is 'a further interference with that fundamental right'.[149] The ECJ found that the Directive limited Article 8 of the Charter on the fact that data retained and subsequently used without the subscriber being informed is likely to generate in the minds of the person 'concerned feeling that their private lives are the subject of constant surveillance.'[150] Proportionality test used in previous case law stated that 'the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.[151]

[146] Digital Rights Ir. Ltd v. Minister for Commc'n et al., 3 I.R. 251, 52 (H. Ct.) (Ir.), (2010); Verfassungsgerichtshof [VfGH] [Constitutional Court], Nov. 28, 2012, ERKENNTNISSE UND BESCHLU¨ SSE DES VERFASSUNGSGERICHTSHOFES [VFSLG], No. 19702/2012, art. 3, p. 1 (Austria).
[147] Id. p. 27.
[148] Id. p. 28.
[149] Id. p. 34 and 35.
[150] Id. p 37.
[151] See S. and Marper v. United Kingdom, (App. Nos. 30562/04 and 30566/04), ECtH.R. (2008). (finding the United Kingdom in violation of Article 8 of the ECHR).

In conclusion the ECJ ruled that the Data retention directive be made 'immediately inapplicable' because it 'exceeded the limits imposed by compliance with the principle of proportionality in light of Articles 7, 8 and 52(1) of the EU Charter.'[152]

More recent cases raising the issue of FDS include *Schrems v. Data Protection Commissioner* (2015), *Roman Zakharov v. Russia* (2015) and *Szabó and Vissy v. Hungary* (2016).[153] In *Schrems v. Data Protection Commissioner* the ECtHR declared void a decision by the European Commission establishing a 'Safe Harbour framework' based on Directive 95/46/EC. This framework had permitted public authorities' access on a 'generalized basis' to 'contents electronic communications'.[154] The ECtHR in *Roman Zakharov v Russia* unanimously held that the Russian system of secret interception of mobile telephone communications was a violation of article 8 of the Convention for the Protection of Human Rights and Fundamental Freedom. Very interestingly, the Court accepted that if certain conditions are satisfied an applicant can claim to be the victim of a violation of article 8 due to the mere existence of a secret surveillance measure. This decision has highlighted the requirements for reasonable suspicion and prior judicial authorization as well as the unacceptable nature of a system 'which enables the secret service and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorization'.[155]

The case of *Szabó and Vissy v. Hungary* concerns Hungarian legislation on secret anti-terrorist surveillance introduced in 2011.[156] The ECtHR held that 'there had been a violation of Article 8 of the Convention.' It did so because it was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. Notably, the scope of the legislation could include virtually anyone in Hungary, with new technologies enabling the Government to intercept mass data easily concerning even persons outside the original range of operation. Furthermore, the ordering of such measures was taking place without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures.

[152] Digital Rights Ireland, Supra note 146, p. 69 and 71.
[153] See Roman Zakharov v. Russia, (Application no.47143/06), ECtHR, (4 December 2015); See also Szabó And Vissy V. Hungary, (Application no. 37138/14), ECtHR, (Judgment) (12 January 2016); See also Schrems v. Data Protection Commissioner (Application no. C-362/14), ECtHR, (Judgment) (6 October 2015).
[154] SPS report Supra note 142.
[155] Ibid.
[156] Szabó and Vissy v. Hungary, Supra note 153.

3.6. Conclusion

This chapter has examined the issue of application of international human rights law specifically the ICCPR and ECHR to the issue of FDS. In doing so it has discussed three different models and approaches towards extraterritorial application. This examination has also taken in to account how FDS programs could fulfill the criteria's of effective control and legality of interference central to the issue of extraterritorial application. After establishing ways to fulfill these criteria's in in the context of FDS this chapter has further assessed current developments by examining recent OHCHR reports and ECtHR (also ECJ) case law. This overall analysis has helped put in to context how the issue of FDS is being dealt in international human rights law and such an inquiry is needed to understanding how the extraterritorial application of the right to privacy is being utilized to deal with the issue of FDS in international human rights law and also to carry over lessons that could be applied to Africa.

Chapter Four:

Application of Existing Human Rights Standards to FDS in Africa

4.1. Introduction

This chapter analyzes the existing African regional and sub-regional legal frameworks that could be applied to govern FDS. It will also assess the possible approach and gaps in these instruments in dealing with FDS. Finally, this chapter will propose applications of the above discussed international and regional human rights principles to help fill the gaps in the existing African regional framework.

4.2. African Data Protection Frameworks

The two most important developments with African regional framework possibly governing FDS are the African Union's Convention on Cyber Security and Personal Data Protection and the African Declaration on Internet Rights and Freedoms (ADIRF).[157] The AUCSDP represents a unique opportunity to address citizens' privacy concerns. Providing a framework through which African states can attempt to regulate cybercrime and enhance the protection of citizen's

[157] See AUCSDP, Supra note 22; See also African Declaration on Internet Rights and Freedoms (2015), (http://africaninternetrights.org/updates/2015/11/article-450/articles); last visited on June 12, 2016.

personal data. This framework can also be applied to solve the weaknesses in the African regional system in dealing with FDS. The ADIRF on the other hand is a regional initiative drafted by a wide array of African civil society organizations. It is a declaration that formulates a comprehensive rights-based framework that contextualizing the various concerns arising from the internet landscape. Critically, it asserts the foundation of internet regulation of openness and freedom, as opposed to prioritizing national security, secrecy and privacy intrusiveness. Being a version of the IPAHRC which could be applied to the Africa, it's a not binding on states. Bearing this in mind this research will focus widely on AUCSDP and other sub regional data protection frameworks.

4.2.1. The African Union Convention on Cyber Security and Personal Data Protection

Before discussing the AUCSDP itself, this paper will first take a brief look at the existing data protection frame works prior to the AUCSDP.

Regional Economic Communities (RECs) were not primarily established to 'foster human rights', but to facilitate a process of 'economic convergence through closer economic and financial cooperation and harmonization policies and programs' only latter was human rights was made a critical aspect of their mandates.[158]

Economic Community of West African states (ECOWAS) is the first REC to adopt a concrete framework on data protection law, adopting the Supplementary Act A/SA.1/01/10 on Personal Data Protection ('ECOWAS Act). [159] This Act was the 'leading initiative' on data protection in Africa[160] and Violation by member states can be enforced by the ECOWAS Court of Justice.[161] Being a supplementary Act to the ECOWAS treaty it may be 'legally binding in creating substantive rights in countries where treaties have direct effect and do not require local

[158] F.Viljoen, "International Human Rights Law in Africa", (2nd ed., Oxford University press, 2012) p. 482.
[159] AB Makulilo "Myth and reality of harmonisation of data privacy policies in Africa", Computer Law & Security Review, Vol 31 (2015), p. 82.; See also ECOWAS Supplementary Act (A/SA.1/01/10, Adopted 16 Feb 2010), (http://www.ecowas.int/publications/en/actes_add_telecoms/SIGNED-Personal_Data.pdf); last visited on June 12, 2016.
[160] Abdulrauf & Fombad, Supra note 20, p. 6.
[161] Makulilo, Supra note 159, p. 83.

enactment.'[162] However, the Act does not provide clear sanction for a member state who fails to transpose the Act in its domestic laws.[163]

The East African Community (EAC) also developed a data protection framework called the EAC Legal Framework for Cyber Laws.[164] Unlike the ECOWAS Act it is not binding on member states and contains recommendations made about reforming national laws to facilitate electronic commerce, to facilitate the use of data security mechanisms, to deter conduct designed to undermine the confidentiality, integrity and availability of information and communication technologies and to protect individual privacy.'[165] The ECA framework doses not "provide any content principles as minimum standards.[166]

The Southern African Development Community (SADC) has its Data Protection Model Law ('Model Law')[167] with an objective of creating a uniform system in the area to protect its citizens.[168] Like the EAC Framework, it is not binding curtailing any potential influence it may have in effective human rights protection in that region.

In 2013, the Economic Community of Central African States (ECCAS) also adopted a model law containing three texts on electronic transactions, data protection, and cybercrime. These texts were adopted by the Economic and Monetary Community of Central Africa (CEMAC) as draft directives.[169]

Cumulatively, with the above initiatives in mind scholars like Greenleaf and Georges assert that "Africa is leading global expansion of data protection law".[170] However, scholars also believe that "the above initiatives cannot be a credible substitute for a continental-wide data protection

[162] G. Greenleaf and M. Georges, "African regional privacy instruments: Their effects on harmonization", Privacy Laws and Business International Report , (2014).
[163] Makulilo, Supra note 159, p. 87.
[164] Draft EAC Legal framework for Cyberlaws (2008) (http://www.eac.int/index.php?option=com_docman&task=doc_view&gid=632&Itemid=148); last visited 27 January 2017.
[165] Ibid
[166] Makulilo, Supra note 159, p. 84.
[167] Southern African Development Community (SADC) Model law, (https://www.itu.int/en/ITU-D/Projects/ITU-EC ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_pro tection.pdf); last visited 27 January 2017.
[168] Ibid.
[169] For detailed discussion of the regional frameworks see Greenleaf and Georges, Supra note 162.
[170] Ibid

initiative" mainly because of the 'limited nature of the jurisdictional scope' of a data protection instrument. [171]

Hence, the AUCSDP has been heralded by some as "potentially the most important development on data protection in Africa."[172] The Convention covers three important areas; Cyber law and electronic transactions, data protection and cybercrime. This paper focuses on only the data protection provisions of the Convention as it is informative to FDS.

The objectives of the AUCSDP is that it commits to 'establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data ' and 'punishing any violation of privacy without prejudice to the principle of free flow of data.'[173] This objective of the Convention shows an unequivocal human rights protection agenda coming out strongly than the other purposes.

Unlike other regional data protection frameworks such as Europe the AUCSDP does not seeks to 'secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his [or her] right and fundamental freedoms, and, in particular, his [or her] right to privacy.' [174] This is problematic leading to the arguments that the Convention is only applicable to only citizen of state parties.[175] However, given that securing the right to privacy is explicitly mentioned as a core objective of the AUCSDP and is applicable to 'any processing carried out in the territory of a state party of the African union'[176] it could be argued that this applies to FDS.

The term 'processing' is defined in article 1 of AUCSDP as 'any collection, processing, transmission, storage or use of personal data by a natural person, the state, local communities, public or private corporate bodies … 'of personal data whether or not by automatic means.' [177] Article 9(d) of the AUCSDP states 'any processing of data relating to public security, defense, research, criminal prosecution or state security' is within its scope, subject to 'exceptions defined

[171] See Abdulrauf & Fombads comparison of the Council of Europe Data Protection Convention with the AUCSDP, Abdulrauf & Fombad, Supra note 20. p. 9.
[172] G Greenleaf & M Georges, "The African Union's data protection Convention: A major step toward global consistency?', Privacy Laws & Business International Report, (2014)
[173] AUCSDP, Art 8.
[174] Abdulrauf & Fombad, Supra note 20, p. 11.
[175] See A Kusamotu "Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by Article 25 of European Union Directive 95/46", Information & Communications Technology Law, Vol 16:2, (2007).
[176] AUCSDP, Art 9.
[177] AUCSDP, Art 1.

by specific provisions of other extant laws and 'data processing obligations' stipulated in section III. This Section of the AUCSDP which is titled 'obligations relating to conditions governing personal data processing' contains six principles.

The first principle is the 'principle of consent and legitimacy of personal data processing.' [178] Requirement of consent may be waived in compliance with a legal obligation by the controller, performance of a public related task, performance of a contract which the data subject is a party and for the protection of the vital interest or fundamental right of the data subject. Consent of the data subject is defined as 'any manifestation of express, unequivocal, free, specific and informed will by which the data subject or representative accepts that personal data is subject to manual or electronic processing.'[179]

The second principle is the 'principle of lawfulness and fairness of personal data processing'[180] in which states parties must provide that processing of personal information 'shall be undertaken lawfully, fairly and non-fraudulently.'

The third principle is the 'principle of purpose, relevance and storage of processed personal data' which states that 'data collection shall be undertaken for specific, explicit and legitimate purposes.' [181] It further contains that the data collection shall be 'adequate, relevant and not excessive towards the purposes for which they were collected and processed.'

The last principle relatable to the FDS is the principle of confidentiality and security of personal data processing where provision is made for processing of personal information to be carried out confidentially especially where the processing involves the transmission of the data over a network.[182]

Apart from these principles data subject's rights are also contained in the AUCSDP. Which include the rights to information, access, object and rectification or erasure;[183]while obligation of confidentiality, security, storage and sustainability of the data controller is also included.

[178] AUCSDP, Art 13, Principle 1.
[179] Ibid.
[180] AUCSDP, Principle 2.
[181] AUCSDP, Principle 3.
[182] AUCSDP, Principle 6.
[183] AUCSDP, Art 16-19 respectively.

Article 14(6) of the AUCSDP provides for rules on trans-border data flows. In which a data controller is prohibited from transferring personal data to a non-member state of the AU except when such a state guarantees 'adequate level of protection of privacy, freedoms and fundamental rights' of persons whose data are to be processed. This rule is, however, not applicable where the data controller requests authorization from the National Protection Authority (NPA) before the intended transfer.[184] This has grave implication especially given that states (as described in programs like PRISM and TEMPORA) share personal information about each other citizens in Trans-boundary surveillance programs. So the term 'adequate' needs to be assessed given transfers are effected to non-member state with an adequate level of protection. While some contend that it the term 'adequate' 'has a meaning informed by the usage of the same term by Article 25 of the European Union's data protection Directive.'[185] Greenleaf argues that "this is very similar to 'adequacy' in the context of the EU data protection Directive."[186] However others state this approach could lead to too much speculation since the AU operates in a totally different region.

When coming to oversight mechanisms, the AUCSDP requires member states to establish institutional frameworks, NPA, to protect personal data.[187] The NPAs must be independent and ensure data processing is carried out in accordance with the Convention. Very robust provision is made for the duties and powers of NPAs which include enforcement, education, auditing, issuance of codes and guidelines and participating in international negotiations. The AU Convention further requires that NPAs must establish mechanisms for cooperation with data protection authorities of third countries.[188]

Another possible stumbling block in the AUCSDP is that it does not limit the right to reservation. This could lead states to disregard parts of the convention that relate to human rights protection focusing on other subject matters like e-commerce and cybercrime.

[184] AUCSDP, Art 14 (6) (2).
[185] Greenleaf and Georges, Supra note 172, p. 2-6.
[186] Abdulrauf & Fombad, Supra note 20, p. 9-12.
[187] AUCSDP, Art 11-12.
[188] Ibid.

Ratification is another problem given the AUCSDP has been adopted in June 2014 and so far no African state has ratified the Convention.[189] Even if the number for ratification is reached states must 'domesticate and comply with their provisions.' This is a problem in Africa as Viljoen notes in bringing 'about compliance with the treaty provisions by governments officials and nationals alike.'[190] It is also worth stating that the AUCSDP does not contain a provision providing sanctions for state parties that do not comply. This According to Makulilo leads member states "who do not establish a framework to definitely undermine compliance level."[191]

Although the AUCSDP has confronted issues of human rights as stated above there are problems faced in its application to FDS. The last part of the chapter identifies ways to bridge this gap using the previously described international and other regional human rights law mechanisms.

4.2.2. The Existing African Human Rights Framework

Many scholars like Olinger *et al* contend that 'privacy was simply not seen as a necessary right for Africans to live freely and peaceably in the current context.'[192] This could mean African leaders will not attach so much importance to the AUCSDP and 'will prefer to rather focus on more contentious human rights issues' which may be the reason for no ratification.[193]

Bearing this in mind it is best to explore a border approach not disregarding the progresses made in the AUCSDP toward FDS governance. This approach is centered on applying the extraterritorial (or universal) reach of international human rights to help fill the gaps in the African regional human rights framework. Given that the African Charter on Human and Peoples' Rights does not contain a right to privacy it would be difficult to fault the ACHPR jurisprudence for not dealing with the issue of FDS directly. As discussed above even other more developed regional and international human rights frameworks have also found the issue of FDS problematic.

Hence a solution could be found in T.S Bulto's description of the 'extraterritorial reach of states human rights duties in the African human rights system', as being possibly applied to foreign

[189] Id, Article 36 provides that "This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification."
[190] Vijoen, Supra note 158, p. 25.
[191] Makulilo, Supra note 159, p. 87.
[192] HN Olinger et al, "Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming Data Privacy Bill in South Africa", The International Information & Library Review, Vol 39, (2007), p. 37.
[193] Abdulrauf & Fombad, Supra note 20, p. 22.

national's within the confines of duties to 'respect, protect, promote and fulfill' human rights.[194] This description in supplemented by Viljoen who indicates "state's extraterritorial responsibility can only be implicated for violations of the African Charter's rights by reasons of 'an extra-territorial incident or event in cases where the State has *de facto* control over that incident or event'.[195] Because of the 'prohibition of discrimination' (equality clause) of ACHPR, a state cannot differentiate between nationals and non-nationals given the AU Charter provides that "Every individual shall be entitled to the enjoyment of the rights and freedoms recognized and guaranteed in the Charter without distinction of any kind such as race, ethnic group, color, sex, language, religion, political or any other opinion, national and social origin, fortune, birth or other status."[196]

The African Commission on Human and Peoples' Rights (African Commission or Commission) also states that "rights under the African Charter are to be enjoyed by all, without discrimination, by citizens and non-national residents alike'.[197] Granted that the Commission is mandated with promotion of 'human and people's rights and ensure their protection in Africa'.[198] T.S Bulto states the Commission 'may receive and adjudicate cases of extraterritorial violations of the Charter's guarantees caused by (in) actions that occur in the territory of any state party to the African Charter."[199]

Cases such as the *DRC Invasion* and the *Burundi Embargo* highlighted this extraterritorial duty of states.[200] Although neither of the cases had 'clear implications for positive duties of a state to residents of third states as none was involved in the relevant litigation'.[201] Given that none of the states objected their 'silence or lack of objection to extraterritorial human rights duties is indicative of state practice' as has been the case in the Inter-American human rights system. [202]

---

[194] T.S Bulto, Supra note 20, p. 249.
[195] F. Viljoen, "Communications under the African Charter: Procedure and Admissibility" ; in M Evans & R Murray (eds), The African Charter on Human and Peoples' Rights: The System in Practice , 2nd ed, (2008)
[196] AU Charter, Art 2.
[197] See Institute for Human Rights and Development in Africa v Republic of Angola 23rd Annual Activity Report (Communication 292/2004 2008), Para 80.
[198] AU Charter, Art 30.
[199] For detailed description see discussions made in T.S Bulto, Supra note 20, p. 260.
[200] See Association Pour la Sauvegarde de la Paix au Burundi v Tanzania, Kenya, Uganda, Rwanda, Zaire and Zambia (Communication 157/96, 17th Annual Activity Report) (2004); See also Democratic Republic of Congo (DRC) v Burundi, Rwanda and Uganda (Communication 227/1999, 20th Annual Activity Report) (2006).
[201] T.S Bulto, Supra note 20, p. 262.
[202] The fact that the U.S. responded to actions against it before the IACHR in the following cases suggested that it accepted that the American Declaration binds the country internationally; See Roach v. United States, (Case 9647,

This is relevant as it shows African states have "assented to be held extraterritorially responsible for their acts as they failed to seize more opportunities than raise their objections'.[203] The Commission has also affirmed that states must abstain from the commission or omission of actions that violate the human rights of individuals and groups in third states.[204]

If an argument is raised regarding the lack of direct stated protection of 'the right to privacy' in the AU Charter the answer may lie in the duty of international assistance and cooperation in regards to human rights. This is in light of that the AU members states pledge 'to coordinate and intensify their cooperation and efforts to achieve a better life for the peoples of Africa and to promote international cooperation having due regard to the Charter of the UN and the Universal Declaration of Human Rights'.[205]

Additionally, states have also agreed 'that fundamental human rights stem from the attributes of human beings, which justifies their international protection'.[206] Granted the ICCPR and UDHR do contain 'the right to privacy' it would be a duty imposed on the AU charter states to respect such a right entailing positive extraterritorial obligations.

The African Charter has established the African commission pursuant of article 30 to "be established within the African Union to promote human and peoples' rights and ensure their protection in Africa".[207]

This entails that the African commission is entrusted with the protection of privacy rights; if this is the case the African commission must utilize all available avenues for protection of such a right. To this end, one of the functions of the commission as stated in Article 45 (c) of the charter is to promote Human and Peoples' Rights by "co-operating with other African and international institutions concerned with the promotion and protection of human and peoples' rights".[208]

Resolution No. 3/87, OEA/Ser.L/V/II.71,doc.9 rev.1), Inter-Am. Comm'n H.R., (1987), p 46-49; See also, e.g., Lenahan (Gonzalez) v. United States, (Case 12.626, Report No. 80/11), Inter-Am. Comm'n H.R., (2011).

[203] T.S Bulto, Supra note 20, p. 262.

[204] Ibid

[205] AU Charter, Preamble, Para 4.

[206] Ibid.

[207] AU Charter, Art. 30

[208] AU Charter, Art 45.

Articles 60 and 61 also highlight how the commission can utilize both African and international human rights instruments and principles in dealing with cases:[209]

Article 60

The Commission shall draw inspiration from international law on human and peoples' rights, particularly from the provisions of various African instruments on human and peoples' rights, the Charter of the United Nations, the Charter of the Organization of African Unity, the Universal Declaration of Human Rights, other instruments adopted by the United Nations and by African countries in the field of human and peoples' rights as well as from the provisions of various instruments adopted within the Specialized Agencies of the United Nations of which the parties to the present Charter are members.

Article 61

The Commission shall also take into consideration, as subsidiary measures to determine the principles of law, other general or special international conventions, laying down rules expressly recognized by member states of the Organization of African Unity, African practices consistent with international norms on human and people's rights, customs generally accepted as law, general principles of law recognized by African states as well as legal precedents and doctrine.

Hence, the reading of articles 30, 45, 60 and 61 points to the fact that the current African human rights framework has 'within' it the possible tools to govern FDS. This means an African regional human rights framework need not stand alone in governing FDS programs rather the researcher proposes that it "draw inspiration" from the AUCSDP (if ratified by AU states) and also institute principles, approaches and case law of the HRC, ECtHR and other international and regional courts to deal with FDS.

4.3. Conclusion

An exploration of the existing African regional human rights and data protection frameworks suggest that there is a reference point upon which Africa can build a lasting framework dealing with the issue of FDS. Instruments like the AUCSDP are indicative the African continent being

[209] Id, Art 60-61.

open to the notion of a regional instrument for governing FDS. Additionally the African charter also serves as a pillar up on which human rights in Africa can be governed and given that several international human rights instruments have identified the right to privacy as a human right it is only fair to assume that the African charter will follow suit. Although, the AUCSDP is not an instrument tailored to governing FDS in the continent it goes a long way in dealing with the issue. As such application of international and human rights principle governing extraterritorial right to privacy will only help the AUCSDP in achieving FDS governance in Africa.

Chapter Five:

Conclusion and Recommendations

5.1. Conclusion

The increased capacity of states to conduct surveillance has shed light on the interests of security and the right to privacy of individuals as significant concepts to dealing with the issue of foreign digital surveillance. As stated by the Special rapporteur on the right to privacy[210] there needs to be a moving away from the debate on "security v. privacy" and a move toward the concept of "security and privacy". This means that security should be viewed as an enabling right for the over-arching right privacy. In order to achieve this balance there needs to be a realization of a viable legal framework both internationally and at regional level governing the issue of foreign digital surveillance. Hence, the central idea behind this research has been the recognition of this viable framework for FDS governance in Africa both in international human rights law and African human rights human rights and data protection frameworks.

The first step in realizing this goal is the understanding of the concept of privacy and establishing its nexus with the concept of FDS. To this end, it is clear to identify how FDS as a form of peacetime espionage conducted by states on foreigners could have an impact on their privacy. As many documented international and transnational mass digital surveillance programs such as PRISM and TEMPORA have shown how states can easily infringe on privacy rights of individuals specifically foreign nationals. This also holds true in Africa, where documented FDS programs are recognized as having implications on enjoyment of privacy rights of Africans.

[210] SRP report, Supra note 141.

Due to the extraterritorial nature of surveillance programs it is essential to disuse the different approaches and models towards extraterritorial application of human rights. Accordingly, this paper has analyze six different models and approaches; such as those which rely on territory to assert application of human rights treaties (Spatial model and the US approach), those who assert extraterritorial application on the basis of physical persons (the personal model) and those which take a protectionist stand towards universal realization of human rights (Protective model and the middle ground).

While these models and approaches reflect the practice of the international community in relation to extraterritorial application of human rights they are not specific to FDS. Consequently the International human rights framework has recently come to terms with this implication of FDS programs on human rights, after revelations by the now exiled Edward Snowden pushed in to action several international human rights organs such as the OHCHR and tribunal like the HRC, ECJ and ECtHR. Although considerable progress has been made by these organs there is still no internationally recognized frame work specifically tailored to dealing with the issue of FDS.

A lasting solution to this problem may lie in applying the already established principles of extraterritorial application of international human rights law towards the issue of FDS. This entails no limitations should be put on the extraterritorial application of the right to privacy as the researcher believes will ultimately prove to be unconstructive. Hence, the ultimate discussion should lie not on the question of applicability of international human rights instruments to the issue of foreign digital surveillance but rather on the substance of an extraterritorial right to privacy. The trend in international human rights jurisprudence also seems to favors this approach as judgments have shown great promise in shaping how international law should view the elements of effective control and legality of interference in extraterritorial application. The principles of necessity and proportionality enshrined in the IPAHRCS also play a significant part in this assessment. However tensions between the concepts security and privacy persist and has even led to some governments continued practice of disproportionate and privacy intrusive measures. Especially documented cases such as PRISM, TEMPORA and quite recent breaking of Encryptions by states are worrying.

In African the recent agreement of a landmark convention on data protection and cyber security has been an encouraging development in the governance of FDS in the continent. It shows that Africa is now ready to move a step further in human rights protection and build a credible information society. However questions should be asked as to how this convention can be applied to govern FDS in Africa. Especially due to the Trans boundary nature of information processing and privacy rights and the additional lack of support in ratifying the AUCSDP proving problematic. While these questions are essential for FDS governance in Africa, it is also worth acknowledging the role played by existing regional human rights treaties such as the AU charter. Cumulatively the AUCSDP and the AU charter, with further utilizing of the principles established by international and other regional human rights frameworks could serve as proper a tool to guarantee the extraterritorial application of human rights (specifically the right to privacy) within the Africa regional human rights framework and in turn be a potential structure to dealing with FDS.

So the researcher proposes that a viable framework for FDS governance in Africa could be found not only by applying the AUCSDP or the AU Charter separately to the issue, but rather cumulatively utilizing the existing international and regional frameworks of human rights and data protection within the context of the right to privacy.

With this in mind the researcher proposes the following recommendations.

5.2. Recommendation

- The current framework of international and African regional human rights law needs a more universal understanding definition of 'the right to privacy' and how can it be better protected in the digital age. This is relevant in regards to understanding the right that needs to be protected and to better define its extraterritorial implications.
- Currently the HRC and especially the ECtHR jurisprudence has had the most developed case law as it relates to foreign digital surveillance and so Africa should needs to incorporate the principles laid down by the judgments of these court as 'inspirational sources' and try to shape its regional and national legislations accordingly.
- African leaders need to understand the importance of data protection mechanisms such as the AUCSDP. So must insure the necessary of the mechanisms by not only to ratifying but also domesticate this convention.

- Governments in Africa must appreciate the fact that they have the responsibility to 'respect', 'protect', 'fulfil' and 'promote' human rights. This applies also to the extraterritorial application of international human right treaties such as the UDHR and ICCPR in guaranteeing the right to privacy.
- As mentioned by the Special rapporteur on the right to privacy the researcher also feels there needs to be a move toward the concept of "security and privacy". This means that security as enabling right for the over-arching right to life and privacy as an enabling right in the overall complex web of information flows need to be consider. So when conducting any FDS programs in the future both international and African leaders need to guarantee that national security dose not impose unnecessary, disproportionate and unwarranted infringements up on privacy rights of individuals.
- Finally a clear relationship must be established between the AUCSDP and international and regional initiatives to govern FDS. In this regard, the AU must also ensure the AUCSDP plays a leading role in steering data protection and privacy rights on the continent as such, regional and domestic initiatives must be consistent with the AUCSDP and regional human rights frameworks such as the AU charter.

Bibliography

Books:

Catarina Krause and Martin Scheinin (eds), International Protection of Human Rights: A Textbook, Abo Akademi University, (2009).

Fons Coomans and Menno Kamminga (eds), Extraterritorial Application of Human Rights Treaties, (Intersentia 2004).

F.Viljoen, International Human Rights Law in Africa, (Oxford University press, 2nd ed., 2012).

Javier García Roca and Pablo Santolaya (eds), Europe of Right: A Compendium on the European Convention of Human Rights (Martinus Nijhoff Publishers, 2012).

Manfred Nowak, U.N. Covenant on Civil and Political Rights: ICCPR Commentary (Engel 2005).

Russell Buchan, "The International Legal Regulation of State-Sponsored Cyber Espionage, International Cyber Norms: Legal, Policy & Industry Perspectives", NATO CCD COE Publications, (2016).

SI Skogly, "Extraterritoriality: Universal Human Rights without Universal Obligations?"; in S Joseph & A McBeth (eds) Research Handbook on International Human Rights Law (2010).

Serge Gutwirth, Yves Poullet and Paul de Hert (eds), Data Protection in a Profiled World (Springer 2012).

Thomas Buergenthal, To Respect and To Ensure: State Obligations and Permissible Derogations; In the International Bill Of Rights (Louis Henkin ed., 1981)

Journal Articles, Law Reviews and Working Papers:

Arthur Gwagwa & Anna Wilton ," Protecting the right to privacy in Africa in the digital age"; paper written as part of the Global Surveillance & Safeguards Project, by Privacy International, IDRC, Canada and their African partners; first published at the Africa Internet Governance Summit, Djibouti, (31 May 2014).

AB Makulilo, "Myth and reality of harmonisation of data privacy policies in Africa", Computer Law & Security Review, Vol 31, (2015).

Alex Sinha, "NSA Surveillance Since 911 and the Human Right to Privacy", Loy. Law Review, Vol 59, (2013).

Ashley Deeks, “An International Framework For Surveillance”, Virginia Journal Of International Law, Vol 55:2, (2015)

Beth Van Schaack, “The United States Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change”, International Law Studies, Vol 90, (2014).

Binoy Kampmark, “Restraining the Surveillance State: A Global Right to Privacy”, Journal of Global Faultlines, Vol 2, (2014).

Chantal Khalil, “Thinking Intelligently About Intelligence: A Model Global Framework Protecting Privacy, George Washington International Law Review, Vol 47, (2015).

Daniel Severson, “American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change”, Harvard International Law Journal, Vol 56, (2015).

Dorothy J. Glancy, “The Invention of the Right to Privacy”, Arizona Law Review, Vol 1, (1979).

Federico Fabbrini, “Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States”, Harvard International Law Journal, Vol 28, (2015).

G. Greenleaf and M. Georges, “African regional privacy instruments: Their effects on harmonization”, Privacy Laws and Business International Report, (2014).

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”, Utrecht Journal of International and European Law, Vol 31, (2015).

John Radsan, “The Unresolved Equation of Espionage and International Law”, Michigan Journal of International law, Vol 28, (2007).

Joergensen, R., “Can human rights law bend mass surveillance?”, Internet Policy Review, 3(1). DOI: 10.14763/2014.1.249, (2014).

Lukman Adebisi Abdulrauf and Charles Manga Fombad “The African Union’s Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?”, Institute for International and Comparative Law in Africa , forth coming article (2017).

Marko Milanovic, “Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age”, Harvard International Law Journals, Vol 56, (2015).

Marko Milanovic, “Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy”, Oxford University Press, (2011).

Oona A. Hathaway, “Do Human Rights Treaties Make a Difference?”, Yale Law Journal, Vol 111, (2002).

Peter Margulies, “The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism”, Fordham Law Review, Vol 82 (2014).

Robert J. Delahunty & John C. Yoo, “What Is the Role of International Human Rights Law in the War on Terror?”, Depaul Law Review, Vol 59 (2010)

Rolf H. Weber and Dominic N. Staiger, “Bridging the gap between Individual Privacy and Public security”, Groningen Journal of International Law, Vol 2, (2015).

Rona & Aarons, “ State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cybrrspace”, Journal of National Security Law &Policy , Vol 8, (2016).

Samuel D. Warren and Louis D. Brandeis, Harvard Law Review, Vol 4, (Dec. 15, 1890).

Sarah H. Cleveland, Embedded International Law and the Constitution Abroad, 110 Columbia Law Review, Vol 110, (2010).

S. E. Wilborn, “Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace,” Georgia Law Review, Vol 32, (1998).

Tara Davenport, “Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis”, Cath. U. J. L. & Tech, Vol 24, (2015).

T.S Bulto,“ Patching The ‘Legal Black Hole’: The Extraterritorial Reach of States’ Human Rights Duties in the African Human Rights System” , SAJHR, Vol 27, (2011).

Graham Greenleaf and Marie Georges, “The African Union’s data privacy Convention: A major step toward global consistency?”, Privacy Laws & Business International Report , Vol 131, (2014).

Tom Burghardt, “Documents Show Undersea Cable Firms Provide Surveillance Access to US Secret State”, Global Research, (18 July 2013).

Will Thomas DeVries, “Protecting Privacy in the Digital Age”, Berkeley Tech Law Journal, Vol 18 (2003).

Newspaper and Press releases:

Charlie Savage, “U.S. Seems Unlikely to Accept That Rights Treaty Applies to Its Actions Abroad”, N.Y. Times, (Mar. 7, 2014).

Electronic Privacy Information Center, "Statement on Council of Europe Cybercrime Convention, Treaty", (26 July 2005).

Glenn Greenwald & Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others", the Guardian, (June 7, 2013).

James Ball, "NSA's Prism surveillance program: How It Works and What It Can Do", The Guardian, (June 8, 2013).

National Security Agency/Central Security Service, 'UKUSA Agreement Release 1940–1956', (24 June 2013).

Press Release, the White House, Office of the Press Sec'y, Presidential Policy Directive/PPD-28, (Jan. 17, 2014).

Paul Farrell, "History of 5-Eyes—Explainer", the Guardian (Dec. 2, 2013).

Orin Kerr, "A Reply to David Cole on Rights of Foreigners Abroad", Lawfare, (Nov. 2, 2013).

International Instruments:

African (Banjul) Charter on Human and Peoples' Rights (adopted 27 June 1981, OAU doc CAB/ LEG/67/3 rev 5, 21 ILM 58, 1982, entered into force 21 October 1986).

African Union Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV).

Report on the Existence of a Global System for the Interception of Private and Commercial Communication, European Parliament Document. no 2001/2098, (July 11, 2001).

African Charter on the Rights and Welfare of the Child art. 2, (opened for signature July 11, 1990), (OAU Doc.CAB/LEG/24.9/49 (entered into force Nov. 29, 1999).

Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, (U.N. Doc. CCPR/C/USA/4, May 22, 2012) U.N. Human Rights Comm., Fourth Periodic Report

ECOWAS Supplementary Act (A/SA.1/01/10, Adopted 16 Feb 2010).

International Covenant on Civil and Political Rights, (adopted Dec. 16, 1966), S. Exec. Rep. 102–23, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976).

European Parliament, Resolution on the US National Security Agency surveillance programmer, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)), (2 July 2013).

European Parliament, Resolution on the US National Security Agency surveillance programs, surveillance bodies in various Member States and their impact on EU citizens' privacy (2013/2682(RSP)), (2 July 2013).

European Convention for the Protection of Human Rights and Fundamental Freedoms E.T.S. No. 5, (entered in to force Nov. 4, 1950).

Resolution on the Right to Privacy in the Digital Age, G.A. Res 68/167, U.N. Doc. A/RES/68/167, (Jan. 21, 2014).

International Principles on the Application of Human Rights to Communications Surveillance, (10 July 2013).

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, (Advisory Opinion 136, 179 on July 9, 2004), I.C.J.

Optional Protocol to the International Covenant on Civil and Political Rights, art. 1, opened for signature Dec. 19, 1966, 999 U.N.T.S. 302 (entered into force Mar. 23, 1976).

Universal Declaration of Human Rights, Dec.10, 1948, (G.A. Res. 217 (III) A, U.N. Doc. A/RES/217III U.N. Human Rights Comm., General Comment No. 31: Nature of the General Legal Obligation on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13, (2004).

Vienna Convention on the Law of Treaties, 1155 UNTS 331, 8 ILM 679, (adopted 23 May, 1969, (entered into force 27 January 1980).

National Legislations:

U.S. Exec. Order No. 12,333, 3 C.F.R. 200, 204–05 (1981), amended by Exec. Order No. 13,470, 3 C.F.R. 218, 227 (2008), (reprinted as amended in) 50 U.S.C.401 app. (Supp. V 2011).

FISA Amendments Act of 2008, H.R. 6304, 110th Cong. (2008).

Reports:

Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, (8 November 2011).

Report on the Existence of a Global System for the Interception of Private and Commercial Communication, European Parliament Document. no 2001/2098, (July 11, 2001).

Reports Submitted by States Parties Under Article 40 of the Covenant, (U.N. Doc. CCPR/C/USA/4, May 22, 2012) U.N. Human Rights Comm., Fourth Periodic Report.

U.S. Dep't of State, Office of the Legal Advisor, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights (Oct. 19, 2010).

U.S. Dep't of State, Office of the Legal Advisor, Memorandum Opinion on the Geographic Scope of Application of the Convention Against Torture and Its Application in Situations of Armed Conflict (Jan. 21, 2013).

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, U.N. Doc. A/HRC/31/64, (March 2016).

Cases:

Al-Saadoon v. United Kingdom, (App. No. 61498/08, 2010) ECtHR.

Al-Skeini v. United Kingdom (Judgment), (App. No. 55721/07, 2011) ECtHR.

Association Pour la Sauvegarde de la Paix au Burundi v Tanzania, Kenya, Uganda, Rwanda, Association for European Integration and Human Rights and Zaire and Zambia (Communication 157/96, 17th Annual Activity Report) (2004)

Bankovi´c v. Belgium (Decision), (App. No. 52207/99, 2001-XII), ECtHR.

Cyprus v. Turkey, (App. Nos. 6780/74 & 6950/75, 2,1975), Eur. Comm'n H.R.

Democratic Republic of Congo (DRC) v Burundi, Rwanda and Uganda (Communication 227/1999, 20th Annual Activity Report) (2006).

Digital Rights Ir. Ltd. v. Minister for Commc'n, (Joined Cases C-293/12 & C-594/12,. I-238, 2014), ECJ.

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

Ekimdzhiev v Bulgaria, (App no 62540/00), 28 June 2007) ECtHR.

Escher v. Colombia, Judgment, (ser. C, No. 200, July 6, 2009). Inter-Am. Ct. H. R.

Jamaa v. Italy, (App. No. 27765/09, 2012), ECtHR.

Klass and others v Germany (Appl no 5029/71, Plenary, 6 September 1978), ECtHR.

Loizidou v. Turkey, (Judgment), (App. No. 15318/89, 310, Sec. A, 1995), ECtHR.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, (Advisory Opinion 136, 179 on July 9, 2004), I.C.J.

Lenahan (Gonzalez) v. United States, (Case 12.626., Report No. 80/11, 2011), Inter-Am. Comm'n H.R.

Liberty and Others v United Kingdom, (App no 58243/00 , , Fourth Section), 1 July 2008), ECtHR.

Lopez v. Uruguay, (Comm. No. R.12/52, U.N. Doc. Supp. No. 40 A/36/40, 1981), U.N. Human Rights Comm.

Malone v United Kingdom, (Plenary), (App no 8691/79, 2 August 1984), ECtHR.

Medvedyev v. France, (App. No. 3394/03, 2010), ECtHR.

Ocalan v. Turkey, (App. No. 46221/99, 2005-IV), ECtHR.

Roach v. United States, (Case 9647, Resolution No. 3/87, OEA/Ser.L/V/II.71, doc.9, rev.1, 1987), Inter-Am. Comm'n H.R.

Roman Zakharov v. Russia, (Application no.47143/06, 4 December 2015), ECtHR.

S. and Marper v. United Kingdom, (App. Nos. 30562/04 and 30566/04, 2008), ECtHR.

Szabó And Vissy V. Hungary, (Judgment), (Application no. 37138/14), (Judgment) (12 January 2016) and (Application no. C-362/14), (6 October 2015), ECtHR.

Weber and Saravia v Germany, (App no 54934/00, 29 June 2006), ECtHR.

Website and Hyperlinks:

http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

http://www.conventions.coe.int

http://www.globalresearch.ca

http://policyreview.info/articles/analysis/can-human-rights-law-bend-mass-surveillance

http://hudoc.echr.coe.int

http://www.lawfareblog.com

https://en.necessaryandproportionate.org/text>

https://epic.org/privacy/intl/senateletter-072605.pdf

http://www.nsa.gov/public_info/declass/ukusa.shtml