Charles University
Faculty of Social Sciences
Institute of Political Studies

Master's Thesis

2017 Alan J. Prijatel

Charles University

Faculty of Social Sciences

Institute of Political Studies

Alan J. Prijatel

The Right to Privacy Deconstructed: International Law in an Age of Virtual Surveillance

Master's Thesis

Prague 2017

Author: Alan John Prijatel
Program: Master's of International Relations (MAIN)
Program Director: Doc. PhDr. Jan Karlas, M.A., Ph. D.
Thesis Supervisor: JUDr. Milan Lipovský, Ph. D.

Submission: 31 July, 2017

Bibliographic note:

PRIJATEL, Alan J. *The Right to Privacy Deconstructed: International Law in an Age of Virtual Surveillance, 72p.* Master's Thesis. Univerzita Karlova (Charles University), Faculty of Social Sciences, Institute of Political Studies: Prague, Supervisor: JU. Dr Milan Lipovský, Ph.D.

Abstract:

In order to understand the process to which the right to privacy operates under current international and regional legal frameworks, we ask ourselves the question if "the digital age" merits an interpretation of privacy unique to this phenomenon of cyberspace. If indeed the right to privacy can be interpreted in this way, we ask whether or not there is a deficit to legal protections to the. This "right to privacy in the digital age" will be taken in context of international law, conventions, principles, and norms in addition to being explored in case-law from the European Court of Human Rights to draw an understanding of the right to privacy in the digital age- if any such right does indeed exist. This thesis essentially, as the title implies, "deconstructs" what puts together the right to privacy and examines what parts of the law that was intended to fortify privacy in the first place, has shortcomings to its defense. I am arguing that there indeed are normative deficits to the right to privacy. In examining key examples of case-law from primarily the European Court of Human Rights, it will be seen if threading apart the important backgrounds of international legal and normative frameworks addresses the function of privacy in the digital age. The International Covenant on Civil and Political Rights (ICCPR) operates separately to the European Convention on Human Rights (ECHR); however, the core of the analysis assesses whether or not such a relationship can be drawn between them and develops an argument of where privacy stands in the "digital age" under this European context.

Keywords: Cyberspace, digital-age, virtual, surveillance, privacy, human rights, international law

Declaration of Authorship

1. The author hereby declares that he compiled this thesis independently, using only the listed resources and literature.

2. The author hereby declares that all the sources and literature used have been properly cited.

3. The author hereby declares that the thesis has not been used to obtain a different or the same degree.

Prague, 31 July, 2017 Alan John Prijatel

Acknowledgements:

The author is principally grateful for his incredibly empowering and loving mother throughout the journey of his master's degree whom he could not have reached this goal without.

Additionally, he would like to thank the Faculty of Social Sciences at Charles University for providing an incredible experience of a master's degree in addition to providing the gracious opportunity to travel between the Czech Republic, Canada, and Australia for his studies in these last two years.

Finally, he would like to thank Milan Lipovský, his supervisor for his thesis, for not only the guidance throughout the entire process, but additionally to the consistent urge to push the limits of basic knowledge by exploring ideas not initially there. The

Institute of Political Studies, Master's Thesis Proposal

Introduction:

From the time of the Peace of Westphalia to the development of formalized international bodies and tribunals, there has been substantial changes to the way the world perceives and translates the meaning of our rights. Today, the claims to challenges to sovereignty continues to exist and we see this ever more prevalent in a world where borders are not only being redrawn, but are being eroded by the infinite boundaries and loopholes of cyberspace. Unseen forces compromise the original assumptions to sovereignty to a point where such a subject matter relies on collective action of nations to address a mutual concern of virtual surveillance for security of human rights, economy, and political legitimacy.

Indeed, Westphalia's implications for state sovereignty presented an interesting debate even foreseen from the times of Hugo Grotius, but today the phenomena is thought to continue to exist within a complex nature comparable to today- especially as it pertains to our privacy rights. The developments from international case law show privacy still possess its classical limits perhaps regardless of the arguments of need to address national security, but still undergoes substantial shortcomings. Given this historical generalization, this has led to the research on privacy rights in the virtual age. The aforementioned classical perception will be used to continue the conversation on privacy where its origins are even more permissible today; much of the scholarly debate finds classical privacy is nothing new to be looked at and modern international law, or norms, should accommodate the realms of cyberspaces in addition to the shifting factual circumstances. Though a shift in the agent, setting, and nation are undergoing processes of change, the embeddedness of our rights isn't. A change in location does not reflect a change in the nature of the right as the origins of rights exists within the individual and not the

agent- as will be explored within the thesis.

Because of this potential theoretical basis for the thesis, there are a few assumed hypotheses:

H1: Within the current academic debate, international organization discussion, and accepted norms, we find international privacy laws and treaties does not adequately reflect the general needs and discourse of the international privacy law community.

H2: Looking further into the current academic debates, and relevant discourse, we do not find any substantial change in the meaning of privacy over the last four centuries of philosophy of human rights regimes.

H3: When we conduct a discourse analysis on the usage of privacy rights in relevant material to be explored (ECHR, ICJ, UNOHCHR, ICCPR, etc.) then it was found little international legislative changes have been adjusted to acclimate virtual surveillance despite the prevalence in the explored material involving cyber-terrorism, crimes against the individual, and mass data collection. The reality of privacy's importance in the prevalence of human rights verbiage isn't addressed to the needs that it deserves.

The aim of the thesis is predominantly to explore this last point; to discover and deepen a better understanding of why privacy is potentially so widely discussed and understood as a right that is credible to human rights regimes, yet doesn't receive the attention to change that it has been argued to deserve. The purpose is to deepen this conversation that is still on the brink of its greater understanding, given the relatively new nature of the matter, and to hopefully unveil better conceptualization of privacy on a widely explored spectrum of privacy rights that the discussion so deserves.

Theoretical Background:

International privacy law operates within a sensitive theoretical framework due to its given nature of human rights implications and the stratified acceptability of how we define such rights across disciplines. In international relations, there are contexts of such rights embedded in how we define the role of the state in its ability to collaborate with other states to address these concerns. Given the intense political debate on the matter, this will only be introduced but not explored to its full extent in this thesis. Furthermore, in analyzing international legal affairs, a different approach will be taken. The notoriety of current international privacy laws and norms has been a hotly discussed debate as to what it means in context of relations with technologically advancing states, the sovereignty of states, and the embeddedness that human rights regimes requires to function.

Marko Milanovic in a recent work on privacy furthered the academic debate that though what may appear as simply the right thing, the right thing often comes at a tremendous cost, a cost of which deviates from the status quo in understanding privacy rights. He further states the necessity of flexibility in extraterritorial surveillance as a requisite for closing this debate further in addition to attaining change in a way that can accommodate the changes of the future. Furthermore, the theoretical background will firstly cross the classical dimensions of natural law as understood by Hugo Grotius where the origin of rights comes from the individual.

Using this brief basis, we will see how such a mindset transcends to today's privacy legal regimes. Thus far, the conversation has been primarily to develop an idea of current treaties and legal frameworks applying to foreign surveillance. By using the current analysis on the matter and the current legal framework on foreign surveillance, the approach of this thesis will attempt

to deepen the debate of virtual surveillance by encompassing a broader academic spectrum of privacy. Indeed, the theoretical basis of the thesis will reflect the current debate, but it will incorporate norms of privacy that have existed throughout history to paint a clearer image of the prominence of privacy in international relations, too.

Working Methodology

Given the dependence upon translation of international legal human rights frameworks, conventions, treaties, laws, and norms, the foundation of this research approach is to delve into available international treaties, international governmental organizations statements, legal discourses, and human rights NGO discourses in order to determine the prominence of privacy as a human right to the international agenda.

Subsequent to extracting this data from these prospective open sources, the information will be used in context of the current academic debate to cyber-privacy given the salient nature of digitization of human communication. This approach ultimately hopes to paint a clearer understanding of not only how certain privacy frameworks came to be, but to demonstrate how they have evolved, and what this means for the future of human rights of privacy during an ongoing process of technological advancement; an unguided trajectory into the indescribable future of our personal lives, and how such an issue greatly effects our views of sovereignty in international affairs.

Working Thesis Structure

1. Introduction
    1.1 Historical Background
    1.2 Purpose
    1.3 Counterarguments
    1.4 Research Questions and Explanations
    1.5 Hypotheses
    1.6 Assumptions and Argumentation
2. Theoretical Framework/Discussion
    2.1 Brief privacy discussion within the Peace of Westphalia
    2.2 Evolution of privacy theory to the twentieth century changes in technology
    2.3 Modern-day perceptions of privacy as a result of the aforementioned to give rise to the current debate on privacy
    2.4 Potentiality for theoretical revisions in the future
    2.5 Theoretical perspective this thesis will use as a foundation for research of the hypotheses, questions, and assumptions.
    2.6 Using the determined theoretical base, the next section follows by looking at Privacy discourse to hopefully unveil more truths to modern approaches to cyber-privacy.
3. Exploring the Relevant Data of Privacy Rights
    3.1 Classical debates and theories
    3.2 International litigation on privacy rights, the UN, the ICJ, and their organs.
    3.3 intergovernmental organization discourse
    3.4 non-governmental organization discourse
    3.5 The spillover of privacy rights from other loci of research: international terrorism, warfare, and security.
    3.6 Academic Debates

4. Data Analysis
    3.1 Making sense of the data holistically
    3.2 Is there a normative understanding of privacy rights?
    3.3 Does each discourse perception reveal any inherent truths to any of the hypotheses

about rights claims, and if so, does this reveal anything important for international privacy legislation?

5. Results
6. Discussion and Personal Reflection of the Results
7. Conclusion
8. Bibliography

Prospective Sources:

Asia-Pacific Economic Cooperation (APEC). “Privacy Framework”. APEC Secretariat, Singapore, 2005. Web.

Anton, Donald K. “The Timor Sea Treaty Arbitration: Timor-Leste Challenges Australian Espionage and Seizure of Documents.” American Society of International Law. Vol. 18, Issue: 6. 26 February, 2014. Web.

Bunch, C.. “Women's Rights as Human Rights, ” in B. Lockwood, Women's Rights: A Human Rights Quarterly Reader, 2006, Baltimore: Johns Hopkins University Press. Print.

Council of Europe. “Details of Treaty No. 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”. Strasbourg, 28/01/1981. Web.

Council of Europe. “Details of Treaty No. 005: Convention for the Protection of Human Rights and Fundamental Freedoms”. Rome, 04/11/1950. Web.

Deeks, Ashley. “An International Legal Framework for Surveillance”. Virginia Journal of International Law. Vol. 55, No. 2. Web.

DeCew, Judith. “Privacy”. Stanford Encyclopedia of Philosophy. 9 August, 2013.

Electronic Frontier Foundation. “International Privacy Standards”. 20 September, 2016. Web.

European Commission. “Protection of Personal Data”. Justice, Data Protection. 29 September, 2016. Web.

European Court of Human Rights. “Personal Data Protection”. Factsheet: Marper v. United Kingdom. June, 2016. Web.

European Court of Human Rights. “Affaire Soria Valderrama v. France”. 26 April, 2012. Web.

Federation of American Women’s Clubs Oversees. “The Right to Privacy in the Digital Age”.

HRC 27 blog, current debates, 2014. Web.

Information Shield. “International Privacy Laws”. Policy Tools: by region. Access 28 September, 2016. Web.

International Association of Privacy Professionals. “IAPP-EY Annual Privacy Governance Report 2016”.

Milanovic, Marko. “Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age”. Harvard International Law Journal. Vol. 56, No. 1. Winter, 2015. Web.

Neill, Elizabeth. “Rites of Privacy and the Privacy Trade: On the Limits of Protection for the Self.” McGill-Queen’s University Press. January 11, 2001. Print.

Organization for Economic Cooperation and Development. “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”. Directorate for Science, Technology, and Innovation: Internet Economy, 2013. Web.

Schmitt, Michael N. “In Defense of Due Diligence in Cyberspace”. The Yale Law Journal Forum. 22 June, 2015. Web.

Superior Court of the State of California. “Fraley v. Facebook”. 11 March, 2011. Web.

Taylor, G.D.S. “The Content of the Rule Against abuse of Rights in International Law.” Web.

United Nations, Office of the High Commissioner for Human Rights. “The Right to Privacy in the Digital Age”. Your Human Rights: Digital Age. Web.

United Nations. “Universal Declaration of Human Rights, Article 12”. Web.

United Nations. “International Covenant on Civil and Political Rights”. General Assembly, United Nations. 19 December, 1966. Print.

United Nations: Educational, Scientific, and Cultural Organization (UNESCO). “Regional Standard-setting Instruments on Women's Rights: Cairo Declaration on Human Rights in

Islam". 5 August, 1990. Web.

United States Court of Appeals for the District of Columbia. "Obama v. Klayman". 28 August, 2016.

Warner, Leif. "Rights". Stanford Encyclopedia of Philosophy. 9 September, 2015. Web.

World Legal Information Institute. "Special: International Privacy Law Library". Web.

Contents:

An Introduction to Privacy:

An essence for the need to address privacy rights in the twenty-first century has been lingering long before discourse flourished on the subject matter. The Human Rights Council Special Rapporteur Frank La Rue on the freedoms of opinion and expression addressed the need for greater attention to human rights as new technologies become more integrated within human's everyday lives.[1] Many may take for granted the extent to which such integration of technology into our personal lives is involved in the evolution and the process of how we interpret human rights. We have touch-screen smart phones, tablets, slim laptop computers, with the abilities to transfer personal information from our finger-tips to screen or keyboard in a matter of seconds. We use such devices to retain our personal information, share it with trusted individuals, or in some instances, share it with individuals, or parties, without even the knowledge of doing so. We browse the internet shopping for clothes, electronics, books, or anything, where search engines are selective our personal data[2], the processes of our thoughts, our human behavior, and transmit this into advertisements in hopes of repeating the processes and collecting more information. The cycle of information collection in the digital age is one aspect of the matter; however, more importantly it is more fundamental to understand how the information is being collected, in what matter, by whom, how much information, where it is stored, how it is handled, whom it is shared with, and, most importantly, if this adheres to the Conventions and international laws on human rights that individuals would hope to posses- if any do exist to be interpreted at a perspective of cyberspace. In the NSA revelations on mass-data collection of telecommunications in also that of metadata as well[3] this only highlighted La Rue's instincts on the matter of human rights in the digital age and became more than a desire, but an inherent calling to fortify a relationship between rights and technology.

---

[1] Chander, Anupam. "United Nations General Assembly Resolution on the Right to Privacy in the Digital Age". *International Legal Materials,* Vol. 53, Issue 4 (2014), pp. 727
[2] CJEU. *Google Spain and Google v. AEPD.* Case, C-131/12. Par. 22. 13 May, 2014.
[3] Cole, David and Federico Fabbrini. "Bridging the Transatlantic Divide? The United States, The European Union, and the Protection of Privacy Across Borders." *Oxford University Press.* ICON, Vol. 14. No. 1. Pp. 221.

This legal analysis assesses the status of the right to privacy in the digital age as it functions via international frameworks. Though many key aspects of privacy in cyberspace will be explored, the principal ideas revolve around the legal process to which surveillance is conducted in addition to the application of that process extraterritorially, and what this means for privacy protections. The main point of the thesis is to gain a greater understanding of the current status of the right to privacy in the digital age and to answer some underlying questions; can the right to privacy be interpreted to include cyberspace? If so, under what legal protections does it exist? Most importantly, what are the current discussions in international law about the right to privacy, in context of surveillance, and what can we understand from the current legal framework on the subject of privacy? I am arguing that privacy, as it is defended in international law and norms, can exist in this way; however, the limitations that exist in international and European law has shown in the key cases to be explored that there is still much to interpreted and acclimated to these new conditions before adequate protections could even be fathomed. In light of the fact that over the last several decades that such a phenomenon has evolved to include more technologies, and thus, more avenues to human rights infringements, there exists this idea that perhaps we can never catch up to advancements in technology that is occurring daily. However, in the international and European interpretation of human rights that we are to explore in this piece, we find that although technologies continue to add new layers to the changing scape of our rights, we feel that this is no different to any other changing phenomenon being applied to other human rights than privacy, and that although these issues are introduced into humans lives, the fundamental basis of these rights do not change.

The inspiration for conducting research on the right to privacy in context of surveillance stems from the United Nations General Assembly resolution 68/167 on "The Right to Privacy in the Digital Age".[4] By not only recognizing here the benefits of global information-sharing, this resolution also highlights the detriment to such a powerful phenomenon; that especially the risk these technologies pose for the livelihood of our rights in cyberspace and potentiality of being susceptible to abuses by not just States but individuals as well. With threats to not only privacy,

[4] OHCHR. "Your Human Rights: The Right to Privacy in the Digital Age". Par. 2. Access: 2 July, 2017.
<http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>

but also the freedom of expression, the discussion of such a matter has only just begun. It is the purpose of this thesis to assemble relevant information that can be applied to "digital" privacy rights as beginning to be explored in resolution 68/167 from the General assembly in context of the ICCPR, to use key case-laws from the ECtHR to develop a comparative understanding on the matter, and to finally discuss our question of whether or not such a relationship between the ECHR and the ICCPR exists.

Lastly, this forwards the Human Rights Council in decision 25/117 to convene a discussion on the "right to privacy in the digital age" in context of extra-territorial surveillance and interception of digital communications.[5] The document presented an overview of the challenges that privacy still possesses in the digital age as it pertains to legal protections and the involvement of business entities in context of such communications.[6] The Human Rights Council concluded in resolution 28/16[7] to appoint a three-year term for a Special Rapporteur, Professor Joe Cannataci, who's mandate gathers, analyzes, identifies, reports violations, and raises awareness to the right to privacy.[8] As a result to the initial resolution on the digital age, it is hoped that this position will enhance the level of protection to privacy in this context and will foster greater research on the subject matter. However, the protection to the right of privacy, and also the greater input of information, is not simply limited to the international level of the United Nations, but of course relies on the implementation and recognition of these rights within the domestic human rights legal frameworks of all. Although a Special Rapporteur adds an institutional position on the right to privacy that provides greater scope to cyber-interpretation of privacy rights, we soon learn that many issues with privacy occur at the European regional level, for the purpose of our study, in addition to within nations themselves.

The underlying framework that the resolution rests is something of key importance and will be introduced in the coming chapters. The International Covenant on Civil and Political

[5] UN General Assembly. "The Right to Privacy in the Digital Age". A/RES/Res/68/167. Par. 11. 21 January, 2014.
[6] Human Rights Council. 28th Session. Sec.1. "Summary of the Human Rights Council Panel Discussion on the Right to Privacy in the Digital age". 19 December, 2014.
[7] Human Rights Council. A/HRC/RES/28/16. 1 April, 2015.
[8] OHCHR. "Special Rapporteur on the Right to Privacy". Access: 14 July, 2017. <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>

Rights (ICCPR)[9] is part of this foundation, which relies on the Human Rights Committee to monitor signatory states regularly[10], in addition to the Universal Declaration of Human Rights (UDHR)[11], and even perhaps the International Covenant on Economic, Social, and Cultural Rights (ICESCR)[12]. Throughout our analysis, we will be focusing mainly on the ICCPR and whether or not the conditions of privacy issues that we shall explore compared to ECHR fall under the interpretations at the international level. Drawing these distinctions will be essential to our hypothesis in that the ECHR does not fulfil the necessary protections to privacy in the digital age that is necessitated by resolution 68/167 with the background of the ICCPR and international law and norms.

Therefore, the focus of the thesis will be on the international and European human rights frameworks under which the right to privacy operates and how this effects the application of the right to privacy today. Given the resolution on the matter, how far and how much has change acclimated to the dimension of rights as we apply them to cyberspace? Is greater discussion and awareness of the matter reciprocated across nation-states? To what extent do some nation's defiance undermine the entire framework of privacy and surveillance altogether? The underlying questions will be of discussion within each chapter exploring the relevant case law of the international and regional courts of discussion. Given the limited scope of privacy in the digital age, the geographic scope of the analysis will generally rest with courts at of course the international level, but predominantly the European level, with only reference to the United States courts as to how privacy would operate under the ICCPR, and of course the ECHR, as a brief comparison to an actor in surveillance and cyber-privacy practice that should not be, and cannot be, ignored.

---

[9] UN General Assembly, *International Covenant on Civil and Political Rights,* 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.
[10] OHCHR. Human Rights Committee. Access: 4 July, 2017 <http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx>
[11] UN General Assembly*, Universal Declaration of Human Rights*, 10 December 1948, 217 A (III)
[12] UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, 16 December 1966, United Nations, Treaty Series, vol. 993, p. 3

We live in a time where technology is involved in our lives in some of the most intimate ways that the founders of the key legislative instruments we are to explore could have never fathomed. With existing in an age where individuals are logging information with everything from the mundane to the most private[13] online, the scope of vulnerabilities when it comes to cyberspace is so wide that it accompanies the need for a wide scope to the protection of privacy as well. These perspectives are understood as a matter that is something that individuals subject themselves to, the involvement of other third parties, where search engines then can be enabled to have information that links directly to that person.[14] The amount of aspects to privacy in cyberspace are indeed wide and it would be impossible to cover every single aspect given the limited scope necessary for analysis which is why we have chosen one of the most salient aspects to international relations. This topic focuses on surveillance practices, the right to privacy, and the interpretation of international and regional convention in context of these practices. Using these, we examine not only the most up to date legislation and case-law, but the foundational cases to surveillance as well, in protecting the right to privacy as it applies to personal data being at risk in surveillance. How is privacy at risk in surveillance, if privacy can even be attributed to exist at all in cyberspace?

Drawing upon the brief history of privacy and electronic surveillance content, we will explore how the key documents on the matter play a role in protecting these rights. We will use this foundation of documents to essentially check-up on the status of international human rights law on the right to privacy in the digital age to determine how exactly such protections, if any at all, are being upheld. There has already begun a conversation about examining the use of human rights treaties like the ICCPR and the ECHR being applied to surveillance and intelligence gathering[15] and we hope that this contribution will be an addition to international human rights law analysis in addition to new perspectives based off of new case law and discourse.

[13] Sisk, Edward P. "Technical Difficulties: Protecting Privacy Rights in the Digital Age". *New England Journal on Criminal and Civil Confinement.* Vol. 42, No. 101. Pp. 103. July 2016.
[14] *Supra*. *Google v. Spain.* Par. 19.
[15] Milanovic, Marko. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" *Harvard International Law Jounral.* Vol. 56, No. 1. Pp.86. 2015.

Before delving into interpretation of the legal framework of privacy in the digital age, it is necessary to establish a command with legal terms that will be of key importance throughout the analysis. The terms are predicated on the relevance to the right to privacy as it applies to cyberspace, but the origins and context of the terms will be established from privacy's physical derivative to the right as well.

I. Defining Privacy in the "Digital Age":

A.) What Exactly is Privacy?

Historically, one of the hardest questions to answer as it pertains to this right is: what exactly is privacy? Given the large context of such a question, it is important for us to establish beyond the philosophical foundation of where the application of this right is stemming from, but to evolve this definition to context of cyberspace, if possible, and how such a definition interacts with the case-law to be discussed.

Given the plethora of privacy interpretations, we can fairly assume that there is no general understanding of privacy in the digital age and that although defining such a concept in principal is possible, much of how the right is applied is circumstantial and varies to the nature of the event which potentially convolutes its meaning. However, this is not to say that having such a complex meaning is necessarily a negative characteristic of privacy, it could be argued that this perhaps deepens its nature of understanding and is important to the changing spheres of knowledge, technology, and polities. Nevertheless, a general output of its understanding is important for moving forward in analysis of privacy in cyberspace. By building a foundation upon which the right to privacy is described at its roots, perhaps distinctions in understanding the role of the term in the treaties and conventions to be discussed will possess more credible logic. There is perhaps the chance that the European Court of Human Rights and the Human Rights Committee observe the defining characteristics of the right to privacy in different ways, and therefore perhaps also terms like "cyberspace", "surveillance", or even "metadata" yet this should not be a limiting factor and should be seen more as a fruitful array potential comparisons

of applying the ECHR and ICCPR to this deeper context of technology. If there is indeed a relationship between cyberspace and the right to privacy, how is this understood in the broad terms of international and regional human rights law and norms?

Privacy, from the latin term "*privatus"* relates to the differentiation from others and entails the individual's ability to exclude him or herself, or the information relating to them, and to be able to disclose said information selectively.[16] Derived from the Louis Brandeis' essay in 1890, this can more simply be understood as "the right to be left alone" from intrusion or unwanted revelation.[17] [18]

Additionally, the notation of "respect to private life"[19], which language is used in the ECHR, perhaps entails a physical component to privacy involving the physical space of an individual regarding the parameters of their own space and prevention of intrusion. Establishing this physical component to the right of privacy is at the roots of the inception of such a right which merits its translation to observe whether or not the parameters of one's personal space can be expounded to the realms of cyberspace.

It should be noted that the ECHR uses the term "private life"[20] while the ICCPR uses the term "privacy"[21]. Although we do not want to convolute the interpretation of privacy any more than it should, these terms could potentially entail differences substantiated enough to merit a difference in interpretation of the case in question. Essentially, this notion of "private life", or even "correspondence", is taken to be interpreted as mail, telephone, and e-mail communications, or telecommunication, which are the inherent mediums to this legal analysis on

[16] Savoiu, Alina. "The Right to Privacy". Annals of the "Constantin Brancusi" University of Targu Jiu, Juridical Sciences Series, Issue 1. Pp. 89. 2013.
[17] Brandeis, Louis D. "The Right to Privacy" *Harvard Law Review*, Vol. 4, Issue 5 , Pp. 193-220. 1890.
[18] DeVries, Will Thomas. "Protecting Privacy in the Digital Age." *Berkeley Technology Law Journal*, Vol. 18, Issue 1. Pp. 286. 2003.
[19] *Supra.* Savoiu. Pp. 89.
[20] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, Article 8, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.
[21] *Supra.* ICCPR. Article 17.

privacy through the European Court of Human Rights.[22] Additionally, the ECtHR interpreted that private life can mean a multitude of things under various situations, and as seen above in court interpretations, with covering the physical and moral integrity of the person[23] and maintaining personal correspondence secretly as it applies to the logging of personal data.[24] However, for the purposes of this analysis, the notion of "private life" will focus only on the aspect of a degree of secrecy of personal correspondence and data in context of surveillance practices. Therefore, for the scope of our analysis, privacy is interpreted as the right to the moral integrity of an individual's personal information and data as it applied to surveillance in the digital age. Although the previous statement allows a foundation and context to move forward with our analysis in should be noted that such a interpretation of privacy, as is implied above, is simply not constant. With new technology intruding into more intimate parts of life, law that attempts to adjust to acclimate to protect the sphere of private life, regardless of being physical or virtual, continues to have difficulty catching up to these advancements.[25]

The ICCPR is the foundation under which the context for the "digital age" was provided in the General Assembly resolution 68/167 "The Right to Privacy in the Digital Age".[26] [27] Privacy is approached in the UDHR and the ICCPR in that:

"no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence…"[28] [29]

[22] ECtHR. *Kennedy v. United Kingdom,* no. 26839/05, 18 May, 2010 Par. 118.
[23] ECtHR. *K.U. v. Finland*. no. 2872/02, B. "The Court's Assessment", 2 December, 2008 Par. 42.
[24] ECtHR. *Ahmet Yildirim v. Turkey*, no. 3111/10, 18 December, 2012. Recommendation III.
[25] *Surpa.* DeVries, Will Thomas. Pp. 285
[26] ICCPR. The international Covenant's broad application to civil rights has proved to be a challenge to the protection of the right to privacy as will be explored later in the discussion of key cases within the Court of Justice of the European Union as well as the European court of Human Rights.
[27] *Supra.* A/RES/Res/68/167.
[28] *Supra.* UDHR, Art. 12.
[29] *Supra.* ICCPR, Art. 17.

In further extrapolation of this right, is that the right to privacy accompanies legal protections of the law against interference and additionally that offline privacy rights are equal to "online" privacy rights in defining privacy in international human rights law.[30] Although this does not specifically define the right, combined with the above defining principles of privacy, it assembles the context under which the right will operate in virtual application moving forward.

However, this does indeed beg one additional question to understanding how privacy is to be interpreted and that is what exactly is meant by the "digital age", "cyberspace", or "virtual space"? Are they necessarily synonymous or do they merit their own respective definitions regarding the context on surveillance? For the purpose of this analysis, given the wide scope of application and interpretation of the term, cyberspace in interpreted generally as the phenomenon of the electronic world created by "interconnected networks of information technology and the information on those networks".[31] The "digital age" as was implied in the resolution and the resolution forward put forth from the Human Rights Council, is the time period at which communication of data through this "space" or domain, through many different avenues of information dispersal such as phone, internet, text, e-mail, to name a few, and essentially highlights the dependency humans have created for these telecommunications technology in their everyday lives.

The right to privacy in context of cyberspace, with the perspective of the CJEU, potentially parallels the respect to personal data; however, this cannot be interpreted restrictively. The relationship that privacy has with "digital" is the concern that "data", or even, "metadata", is the object of privacy that is at risk in the explored context of virtual space. Surveillance in context of data should be interpreted to include the "compiling, administration, and the use of large datasets, passing on of datasets for purposes other than legitimate ones, assembling and harvesting metadata…" Furthermore, we can establish that data is then personalized information that has been input into digital form an individual uploaded onto the internet- whether that be for locational, or any other identifiable purpose. Although aspects of the extent to which data is attached to identity and what is indeed sensitive information varies from the CJEU and the

[30] *Supra.* A/RES/Res/68/167, Par. 3.
[31] Government of Canada. "Canada's Cybersecurity Strategy. Pp.2 2010.

ECtHR, they do possess certain commonalities such as they both examine interferences to the right to privacy in the processing of personal data [32] and that this process is subject to the collection of information in only that it is "necessary."[33] This general aspect is important for understanding the case-law in the coming chapter; however, given the unique scope of both the ICCPR and the ECHR, there will indeed be differences substantiated enough from simply observing the direct statements approaching "privacy" or "private life" as was explored above.

B.) What is Personal Data?

Finally, the last important detail pertains to vessels under which information is stored, and thus how it is extracted, which further begs the question as to whom has access to perform such actions on data or simply access to data altogether. "Personal Data", in the perspective of the Council of Europe, in addition to the exact definition from the European Parliament and Council of the European Union[34], however as a general definition that can be applied widely, means "any information relating to an identified or identifiable individual."[35] Therefore, it is fair to assume that, in some form of the process, the information that an individual deems as unique to the identity of themselves, was therefore transferred from such a physical existence to virtual existence- if we are to apply the simple notion of what data is and how this is connected to our definition of "digital" or "cyberspace" as per the understanding and context of our analysis. The definition that the European bodies listed above provides us with what "personal data" can mean but what it does not provide information about is whether or not this information came directly from the individual or if it is information that is attached to the identity of a person but was retrieved elsewhere. There are infinite means at which information could possibly be attached to an individual which could include identification numbers that perhaps companies, banking,

[32] CJEU. *Digital Rights Ireland Ltd v. Minister for Communications and Others*. Joined Cases C-293/12 and C-594/12. Par. 32. 8 April, 2014.
[33] Ibid. Par. 32.
[34] European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995.
[35] Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, Art. 2. 28 January 1981, ETS 108.

personal electronics, accompanies that person yet could be information that is vulnerable because of little known fact that it is in anyway connected to that individual.

Personal data, in the perspective of the ECtHR, should only be available to those authorized by the law to have that data, with consideration to the covenant, and should only be information that an individual can ascertain what information is being held, who is controlling that personal data, for what reasons, and should have "the right to request rectification or elimination".[36] Similarly, in the *Google Spain v. Spain* case, they highlight Directive 95/46[37] of European Law which also provides rights to rectification of information that does not comply with the Directive in the context of automatic storage of information from search engines.[38] Resolution 68/167 specifically draws the correlation between the surveillance of personal data and the violation to the right to privacy and freedom of expression[39] reaffirming that sensitive information is indeed encrypted to virtual form and that there is a need to establish safeguards and protections to uphold the right to privacy in this context.

Of course, like the definitions above, each of the bodies that will be explored in case law may approach the terms that we are describing in their own way which may make it difficult to generalize the concepts we are trying to establish beforehand. However, giving an idea of the greater conceptual definitions of what we are discussing is hoped to at least provide a foundation going into the analysis of various legal perspectives on the matter of privacy in the digital age.

[36] *Supra. Yildirim*. Par. 10.
[37] *Supra.* 95/46/EC.
[38] *Supra.* Google Spain. Costs (1).
[39] *Supra.* A/RES/Res/68/167, Par. 2.

C.) Defining "Surveillance" in context of privacy.

Surveillance in the ECtHR can be interpreted to include "telephonic, telegraphic, wire-tapping and recording of conversations" in context of mediums that are questioning the legitimacy of its purposes.[40] Although this interpretation is derived from the ECtHR, in the analysis these are the most common forms of correspondence, in the ECtHR, the CJEU, and the Human Rights Committee, that will be connected to the right of privacy in context of the digital age- even though to the latter court and committee may present a different understanding to the degrees and methods "surveillance" may be understood. In the context of the Human Rights Committee, "interference" has a relationship with "interception" where in General Comment No. 16 it is stated that "correspondence should be delivered to the addressee without interception and without being opened or otherwise read."[41]Additionally, "foreign" surveillance could also be understood as directing surveillance towards individuals, official or not, of foreign governments, against foreign nationals generally, or simply individuals outside of state territory that could be a national but not necessarily[42] which therefore under this perspective could fairly be assumed that this is an action of collecting information, whether covert or not, of information of individual that are foreign nationals or outside the territory. This begs to question how the interpretation of foreign surveillance would apply under Article 17(2) of the ICCPR in addition to Article 8(2) of the ECHR; however, such a concept will be further explained in the chapter on extraterritorial surveillance.

Moreover, this is a general understanding of surveillance, and overall its connection to personal data and thus privacy, but in order to truly understand its definition, analyzing the context at which it was applied will provide a more adequate description for its relevancy to privacy and thus a definition of surveillance within that judicial body. Nevertheless, "surveillance" in its general definition in light of the context provided above in which it could be applied, will be understood as a clandestine operation, or method of intelligence gathering, by an individual or state for gathering information on a selected individual or group, which to some

[40] *Supra. Yildirim*. Par. 8.
[41] HRC. General Comments, A/HRC/RES/28/16, No. 16. 4 January, 2015.
[42] *Supra.* Milanovic, Pp. 86.

extent involved interception of personal information, and may or may not include interference with the individual's rights. The extent to whether the measures were conducted under "secret surveillance", as in the case law to be seen, will be an important legitimating factor for the State in question, or whether or not the information collected fulfills the context of "personal data" as we explored above, begs a different question on the application of the matter. Both the secrecy of the surveillance and the content of the surveillance are key aspects with the ECtHR case law that warrants deeper investigation- especially in how their interpretations could play in application of international law and the ICCPR.

i.) What is Metadata?

Generally, metadata in its simplest understanding is to be understood as "data about data" as it is the information about the processes, purposes, and methods involved in the extraction of the data.[43] In greater context of its understanding, metadata provides detailed aspects into the collection of that particular information which could then possibly be used into determining greater details as to the individual in question specific ways of life. In the dissenting opinion of Judge pinto de Albuquerque in *Barbulescu v. Romania* it was argued that Convention principles apply to the protection of not only the content of the communication but also the "metadata" that it accompanies as it "may provide an insight into an individual's way of life, religious beliefs, political convictions, private preferences and social relations."[44] Additionally, metadata could encompass what is understood as "further information" of which the conditions of the interception occurred where certain data unveils a compilation of characteristics to the interception that could include but is not limited to the time the interception occurred, the location, the equipment that it was used, whether computer files on the data was created, accompanying e-mails, or even text messages.[45] Therefore, given the connection to personal data and information, metadata could potentially warrant the need for the protection of privacy

[43] Australian Bureau of Statistics. "Statistical Language: What is Metadata". 3 July, 2013. Web. < http://www.abs.gov.au/websitedbs/a3121120.nsf/home/statistical+language+-+what+is+metadata>

[44] ECtHR. *Barbulescu v. Romania.* no. 61496/08, Dissenting Opinion, Justice Albuquerque. Par. 5. 8 April, 2014.

[45] ECtHR. *Szabo and Vissy v. Hungary.* no. 37138/14. Par. 68. 12 January, 2016.

beyond just the simplified "data" but everything else that goes in to that process. Metadata, therefore, illustrates the modern interpretation and issues with data that we perhaps unique in the digital age.

Whereas, the process of data collection, in the past without a "virtual age", did not possess the technology to group these processes, and step by step information, and create statistical tables to draw inferences based on the information, metadata essentially exponentially multiplies the responsibilities of the protection of privacy is beyond the fragment of the personal information at hand, but is everything connected within that process that is relevant as well. The question stands as to whether we can apply the ICCPR and the ECHR to metadata, or if even interpretation of these treaties are sufficient to the safeguard of the personal information within those documents.

ii.) Extraterritorial surveillance

When this point on surveillance applies to extraterritorial application, which could be interpreted within the context of collecting correspondence or data on a territory not within jurisdiction of the involved party, hopefully a similar collaborative approach could be thought of in order to draw distinctions of its general concept of application; however, defining the way each body defines extraterritorial application of surveillance will hopefully illuminate the inherent legislative weaknesses. It should be noted that "extraterritorial" is different than the term in international law "extraterritoriality" which is immunities to the jurisdiction of the state officials and international organizations are present.[46] Because of how close the terms are, drawing a distinction beforehand will settle any confusion while using the term in the interpretation of international law.

Moving forward, to cover the basics of extraterritorial application in cyberspace, it is possible for one to draw conclusions as to what the term means just by separating the prefix "extra" with the suffix "territorial" and how they intermingle within linguistic analysis. Given

[46] Encyclopedia Britannica. Extraterritoriality. International Law. Access 22 July, 2017.

this generalization, some define "extraterritorial surveillance" as one of the derivative terms to the general term "foreign surveillance", to mean a clandestine intelligence gathering method of communication surveillance taking place entirely overseas.[47] Using this definition, we can perhaps assume "extra" means anything but inside of the "territory", as crossing jurisdictions and territories can of course occur more than just across the sea, and this analysis is much underprepared to apply the United Nations Convention on the Law of the Seas (UNCLOS)[48] to the application of surveillance using water-borders. However, we must digress, the most important aspect therefore can be concluded is that extraterritorial for the interpretation of our analysis is an action that occurs outside of the jurisdiction and/or territory of the State in question.

D.) Using these interpretations in the "digital" age

One of the most important contexts that was described above which is of particular use for this analysis is the protection and right to correspondence- as this protection to privacy was developed under context of virtual surveillance.[49] Although the background to privacy possesses fundamental situation differences, application of the said definition will hopefully prove to make analysis more useful.

This information provides the context necessary to set the stage for the analysis of the right to privacy in the digital age and will be important for further understanding the status at which the right to privacy operates in cyberspace and what we have learned from case-law up until this point.

[47] Deeks, Ashley. "An International Legal Framework for Surveillance." *Virginia Journal of International Law.* Vol. 55. Pp. 400. 2015. Web.
[48] UN General Assembly, Convention on the Law of the Sea, 10 December 1982.
[49] *Supra. Ahmet Yildirim v. Turkey.*

III, Case Selection:

When searching for cases, some specific language a search tools were used in order to find what we are looking for in context of the analysis. For the European Court of Human Rights (ECtHR) only cases that involved Article 8-1 of the European Convention for Human Rights (ECHR) were searched upon with also funneling down the case-law pool via searches for surveillance, resolution 68/167, the digital age, and the like terms. Problems that encountered in searching cases on HUDOC (the ECtHR case-law database) included that the term "digital" although used in our case, was used several times in order to address a different principle from the Human Rights Council called the "digital divide"[50] [51]

Many of these cases are well known in the international privacy and data law legal and scholarly communities; however, there are many cases that have simply been too new to include in any relevant analysis. Using these well-known cases, in addition to the newest ones, we hope to draw an approach to the right to privacy that presents why the right to privacy, establishing those rights, securing those rights, and monitoring those rights, is such a complex issue in the twenty-first century and how the matter is only growing deeper into the international legal web of internet and telecommunications law. This furthermore will be explored into the fundamental core of our legal analysis: whether, and how, if possible, the conclusions we have draw about digital privacy under either the CJEU or the ECtHR, can be applied to the Human Rights Committee, under international law and norms via the ICCPR. Essentially, a comparative analysis on the ICCPR's functionality to the response to digital privacy rights issue at the European regional, legal, and normative levels.

When it comes to the European Court of Human Rights (ECtHR), the general examination of our application of privacy virtually in case-law, the predominant case used was *Roman Zakharov v. Russia*[52] as it was newest case on the application of surveillance and how article 8 of the convention falls in to this. This case sites similar case law under the convention

[50] ECtHR. *Kalda v. Estonia.* no. 17429/10. 19 January, 2016.
[51] Human Righs Council (A/HRC/17/27). Special Rapporteur. 16 May, 2011.
[52] ECtHR. *Roman Zakharov v. Russia*. no. 47143/06. 12 January, 2016.

within the ECtHR, and even some mentioning of case-law from the CJEU. Using this case a general foundation for the latest approach to privacy in cyber-space, other cases will be referenced as well as they become relevant; however, although this case may be argued as not the most important, it certainly is a key player in understanding whether or not there is indeed a deficit to to the international legal protections to privacy as it pertains to surveillance in the digital age. Due to the fact that the ECtHR operates as the human rights judicial body of the Council of Europe, as said before, the geographic scope is unfortunately limited. Nevertheless, the plethora of case-law extracted from the ECtHR and the CJEU will be assessed to determine the universal context of privacy in cyberspace via the normative framework of the ICCPR.

IV, Current Legal Framework of Privacy: International and Regional Law

Resolution 68/167, as the principle resolution on the right to privacy in the digital age, states the purposes and principles of the Charter of the United Nations, the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the International Covenant on Economic, Social, and Cultural Rights (ICESCR), and the Vienna Declaration and Programme of Actions are the key foundational international documents under which the right to privacy in the digital age was inspired or reaffirmed.[53] This first section utilizes this resolution as the background of this analysis.

The forthcoming documents, resolutions, and conventions of which will be explored for this study are pertinent to the understanding of the case law to come. For this reason, key legislation and documents from the United Nations, generally, the Human Rights Council, the Council of Europe, and the European Union, will briefly introduce the legal foundation upon which the following case-law rests upon. Each of the documents has an inherent role to the approach of surveillance today, and in order to understand this concept under the international and European regional perspectives, these documents clearly define, contextualize, and highlight

[53] *Supra.* A/RES/Res/68/167.

the components of privacy, data, and surveillance applied to international and regional conventions. In placing international law in juxtaposition to European conventions, as stated within our hypothesis, there is potential to draw distinctions to the legal safeguards to privacy; however, there is also the potential that such there exists some parallelisms as well which is hoped to be defined in exploring the relevant institutions.

A.) United Nations

The United Nations has reaffirmed in many key foundational documents of the right to privacy as a principal and innate human right. This right is enshrined in the Universal Declaration of Human Rights (UDHR)[54] in addition to being repeated and reaffirmed in the International Covenant on Civil and Political Rights (ICCPR)[55] *verbatim* to the former document. Article 17 states:

> "1. *No one shall be subjected to arbitrary or unlawful interference with his* ***privacy****, family, home or* ***correspondence****, nor to* ***unlawful attacks*** *on his honour and reputation. 2. Everyone has the right to the protection of the law against such* ***interference*** *or attacks."*[56]

Having established the relevant components of the UDHR, and thus the ICCPR, the United Nations General Assembly resolution 68/167 contextualizes the right to privacy in a more specific manner. The rapid advancement of technology has "enhanced the capacity of governments, companies, and individuals, to undertake surveillance, interception and data collection, which may violate or abuse human rights"[57]. It further states that "no on shall be subjected to arbitrary or unlawful interference"[58] in also that "the right to privacy is important for the realization of the right to freedom of expression and to hold opinions without

[54] *Supra.* UDHR.
[55] *Supra.* ICCPR.
[56] Ibid. Article 17
[57] *Supra*. A/RES/Res/68/167. Par. 2
[58] Ibid. Par. 3

interference…"[59] The document holds that individuals should be able to have the freedom to access information as a part of democratic participation and expression, and any arbitrary and unlawful collection of personal data is a "highly intrusive" act to privacy[60]. However, as the right to privacy is indeed an inherent right, the document does provide a necessary loophole to privacy for purposes of national security and public safety. It states that reasons for public security may justify gathering personal information but that this must be done under obligations in international human rights law.[61] The resolution also stresses the importance of understanding the negative implications of extraterritorial surveillance and interception of communications even when conducted in mass scale. [62] Moreover, there are many aspects to the resolution that are of interest for the purpose of our analysis.

The key aspects of the resolution that are important for this study, and our hypothesis, includes the elements of surveillance as potentially arbitrary, and thus the process of interception at which a state justifies its actions, the loss of privacy for legitimate aims of security, and the negative aspects of extraterritorial surveillance- including in mass scale. These characteristics of the resolution potentially highlight the inherent privacy issues as applied in the case-law to be examined. Can it be justified that the right to privacy does indeed exist anymore when states can circumvent the rights of individuals for purposes of national security or when individuals willingly, or arbitrarily, have personal information more than just surveyed, but extracted, stored, and utilized without their knowledge? Is it enough to say and recognize, as is demonstrated in the resolution, that review of states national legislation, greater safeguards, and recognition of the potential violations to human rights extraterritorial surveillance, including mass scale, is sufficient for the protection of privacy? Although case-law is limited in reference to the resolution because of how new it is, applying principal of the right to privacy in context of surveillance and this resolution will aid in developing a position of privacy protections in the digital age.

[59] Id.
[60] *Supra.* A/RES/Res/68/167. Par. 5
[61] Ibid. Par. 7
[62] Ibid. Par. 8

B.) The Human Rights Council

In resolution 68/167, as per the request of the General Assembly, the Human Rights Committee invited the Human Rights Council to write a report on "the right to privacy in the digital age"[63]. This report not only details the background and motives of the resolution but additionally examines fundamental issues with privacy. The Human Rights Council reaffirms the components of the resolution but also includes the challenges to privacy that will be highlighted in the following chapters. The components include the right to protection against arbitrary or unlawful interference with privacy or correspondence, defining "arbitrary" or "unlawful", the role of the law in privacy in surveillance, who is protected, procedural safeguards, and the right to effective remedy.[64] This report from the Human Rights Council will be drawn from as the analysis progresses because each play a role in the protection of privacy in virtual application and will aid in determining the extent to which there exists a legislative deficit to privacy and surveillance in the digital age.

C.) The Council of Europe

Perhaps what will be the most sourced legal instrument throughout this analysis, which has already been mentioned, is the European Convention on Human Rights[65]. Of course, the context of our analysis pertains to the right of privacy and as such, the Article with the most involvement within the case-law for surveillance practices is that of Article 8. Article 8 states:

*"1. Everyone has the right to respect for his **private** and family life, his home and his **correspondence**.*

*2. 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*

[63] *Supra*. A/RES/Res/68/167Par. 5.
[64] Human Rights Council. "The Right to Privacy in the Digital Age: Report of the OHCHR". 3 June, 2014.
[65] *Supra. ECHR.*

prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[66]

The entirety of the analysis will, as said, continuously reference this Article in especially the notion of private life, correspondence, in the first Article, and in accordance of the law, and necessary in a democratic society, within the second Article. Our hypothesis believes the language and interpretation of the ECHR, as stipulated in Article 8, does not meet sufficient practices of privacy as would be protected by the Human Rights Committee under the ICCPR.

In ETS 108 of the Council of Europe, personal data is to some extent protected within this document as the only binding international legal instrument of its kind.[67] The convention puts first and foremost the protection of personal data in relevancy of preserving the right to privacy[68] by stating automatic data processing must be obtained fairly, lawfully, stored for legitimate purposes, is relevant, accurate, and is only used for a certain amount of time that is required.[69] It also establishes that an appropriate measure of security and safeguards are necessary for the protection of personal information from abuse; where the controller of information is located, to have reasonable time to have confirmed if personal data is stored in an automatic data file, in addition to obtaining rectification if data processing was contrary to domestic law.[70] There also includes the need to address that automatic processing of personal data can be permitted in the interest of the protecting state or national security or protecting the freedoms and rights of others.[71] Overall, with these being the most relevant articles in the Convention for the purpose of our analysis, it can be seen that, at least within the Council of Europe, there appears to be legislation that is in place in order to protect the personal information of individuals which will be necessary to the deepening our understanding of data privacy within the case law of the ECtHR.

---

[66] *Supra.* ECHR. Art. 8.
[67] Council of Europe*, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 28 January 1981, ETS 108.
[68] COE. No. 108, Art. 1
[69] Ibid. Art. 5.
[70] *Supra*. COE, No. 108, Art. 8
[71] *Supra*. COE, No. 108, Art. 9

In piecing together these articles, there are commonalities between the language expressed within this document, to the detailed reports from the Human Rights Council, and even with the resolution 68/167 from the UN General Assembly. Nevertheless, although certain bodies share similar discourse on the matter, the nature of their governance systems are all different and thus the binding qualities of such statements are different as well. Resolution 68/167 *encourages* states to recognize the effects surveillance could have on privacy in the digital age and is more of a calling to member-states to recognize these rights during this new era. In contrast, the Convention listed from the Council of Europe is a binding document to the State signatories of the Convention. Having said that, there appears to be agreement that states must review their procedures on the processing of personal data and that the right to privacy needs to be addressed in a matter of surveillance during a time of increased and advanced technologies.

Nevertheless, in line with the principles of the hypothesis, I believe that the ICCPR stands to protect the rights of individuals in the digital age greater so than the ECHR despite the documents binding qualities to members of the Council of Europe. The reasoning behind such a hypothesis lies within the procedure, verbiage, and approach to privacy in specific, with relation to surveillance practices, the the Human Rights Committee under the ICCPR presents in discourse in addition to the widespread applicability of international law within that scope as well.

i.) The European Court of Human Rights

Although the above documents, especially the ICCPR, provides a wider international scope to the right to privacy in context of our analysis, there also is a need to address European Conventions due to the inherent nature they operate within the European Court of Human Rights. The ECtHR will play a vital role in understanding the application of privacy safeguards as explored above so our analysis would be incomplete without at least an understanding of how personal data protection functions at the European regional level. The ECHR is the principal document that the ECtHR bases the relevant case-law that will be explored in the next chapter off of; however, the Charter of Fundamental Rights of the European Union (CFREU) is also

relevant to privacy's application at the European level as well, as mentioned in UNGA Resolution No. 68/167, under Article 7 on the "respect for his or her private life."[72]

The European Court of Human Rights determines whether or not there have been violations to the Convention, and if so, under what grounds and context that this was taken. The cases in the following chapter were all involved to a certain extent as to whether Article 8, as stated earlier, possessed any merits in that especially to the right of "correspondence" within the Article. The law does not state, or specify, "surveillance", or "unlawful" interference, in how the ICCPR directly states; however, Council resolutions and directives from the level of the European Commission contextualize interception of telecommunications in a way that is, perhaps even more intelligible, than under international frameworks but nevertheless some are non-binding, where case-law has had no trouble addressing surveillance, unlawfulness, and interception practices under the interpretation of Article 8 in addition to the background in European law without such specific terms. Moreover, an omission of "surveillance" or "unlawful" interference under Article 8 does not appear to be a hindrance in addressing such such concerns within the ECtHR.

D.) Law of the European Union

The Council of the European Union introduced a resolution that specifically addresses the lawful method of intercepting telecommunications[73]. It outlines the responsibilities of Member States for the needs of "competent authorities" to conduct the interception in manner that recognizes the respect for privacy enshrined in the "territorially applicable national law". Although there is no mentioning of international standards, norm, or even the ECHR on the right to privacy, it can be assumed that these documents play an inherent role as a resolution from the Council from the E.U. Additionally, the emphasis to "national law" is perhaps to encourage states to uphold the need to respect privacy in national law given the vital role domestic law plays on interception of telecommunications.

[72] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02.
[73] European Union. *"*On the Lawful Interception of Telecommunications" Council Resolution 96/C 329/01. 17 January, 1995.

Later the same year as the above resolution, the European Parliament and the Council of the European Union issued a directive that specifically addresses the "processing" of personal data and the "free movement" of data as well.[74] Directive 95/46/ EC has a primary objective of processing personal data in a way that keeps in mind the importance of fundamental freedoms and privacy enshrined in the Charter of Fundamental Rights the European Union[75] and the ECHR. The document outlines the lawful methods of the processing of personal data on quality, freedom of expression, the rights to data, and security of processing, to name a few. Each member state is expected to be upheld to these provisions on data processing through European Law and since this time, further cases and resolutions highlight the evolving political, technological, and economic context of the situations to accommodate privacy. Such evolution that includes "new electronic communications service" and even new "digital mobile networks"[76] is enshrined in new directive that contextualize the situation of technological advancement, as was seen here, to address telecommunications providers pertaining to the processing of personal data or information in new public communications networks. The aforementioned directives aided in the construction of the 2006 Data retention directive providing scope to Member States on attempting to align respect of privacy with data retention for "the purpose of investigation"[77] where the most up to date regulation on protecting personal data, on the free movement of data, repeals the General Data Protection Regulation , which was described earlier, in the hopes of rectifying "legal uncertainty"[78] associated with the risks involved with personal information and online activity. The extensiveness and detail that this document possesses covers everything from the lawfulness of processing personal data, the rights of individuals and states with the data involved, the correct authorities to be consulted and that are under control, and specific details under the restrictions "that are necessary and proportionate measures in a democratic society to safeguard"[79] which could be national security and preventing abuse of data retention. It should be noted that the document never states

[74] *Supra.* Directive 95/46/EC.
[75] *Supra*. CFREU, Art. 8.
[76] European Union. Directive 2002/58/EC, Par. 5 31 July, 2002.
[77] Ibid. Par. 4.
[78] European Union. Regulation 2016/679 Par. 9. 27 April, 2016.
[79] Ibid. Art. 23.

"privacy" as to be protected, but "observes" the freedoms and rights enshrines in "the Treaties" specifying "the respect for private and family life"[80]

D.) Note on Domestic Legislation

Domestic legislation, when and if available, will only be mentioned as an aside to help describe the context of the international or European conventions in place, or the case-law that is being discussed. Given the varying interpretations of domestic law, therefore, it will only ever be used in a supplementary manner that illuminates potential concerns with the right to privacy in helping explain why, perhaps, that there is such an issue with states not upholding their responsibility to this human rights.

Throughout the exploration of the relevant legislation that is relevant to the protection of privacy in the digital age, there were some common characteristics within conventions, international law, and domestic law, that were put established for the hope of preserving human rights as it pertains to privacy and personal data. These components involve the safeguarding of personal data, the use of personal data for legitimate purposes, the arbitrary use of personal data, and even extraterritorial application of collecting personal information- whether or not that this was conducted in mass form. These aspects of clandestine intelligence gathering, under surveillance from a state or individual actor, are what will be explored in the next chapter. These have been chosen as subjects within personal data collection in hopes of revealing what issues in protecting privacy in surveillance practices still continue to be a problem if such a problem does exist.

[80] *Supra*. 2002/58/EC Par. 6.

V, The Action of Interception at the Core of Privacy Issues

In all of the explored cases from the European Court of Human Rights (ECtHR), extension of the violation of the right to private life under article 8[81] were under allegations that the party in question had communications that were being intercepted. What can be assumed lies at the core of privacy rights as it pertains to telecommunications is understanding the process of interception of those communications, who was afflicted by such interceptions, how, and to what extent, provides a deeper context to privacy that could aid in discovering whether or not there indeed exists a deficit to legislation and international protections of the right to privacy in the digital age.

Therefore, the purpose of this chapter is to deconstruct the assemblage of the procedures of interception in order to discover whether or not this is where the weak-link exists to the protection of privacy in cyberspace. The action of "interception" perhaps sounds intrusive, in any general sense of the definition, which could be the reasoning why an individual would feel such an action, regardless of being physical or virtual, is an infringement upon their rights. The right to privacy, as was stated in the definitions chapter, was partially created to address the physical space, or physical objects, of privacy that are attached to privacy; however, this era of the "digital age" has provided a multitude of communications technologies such as the internet, cell phones, texting, Snapchat[82], or even Instagram,[83] to a point that the possibilities of interception of information has well-multiplied beyond any general physical interpretation. Having said that, there stands the question of whether or not there should be any differentiation to the interpretation of interception in being virtual or physical. In principal, we believe that such a differentiation is not necessary for interpreting privacy; however, because the context of the manner in which interception is now conducted due to advancements in technology, this warrants a need to provide adequate legal protections to privacy in the procedure of interception. Some laws within the procedures of interception, collection of information, or surveillance, under the ECHR, Article 8, appear broad in principal and interpretations have been widely circumstantial.

[81] *Supra*. ECHR. Art. 8.
[82] Snapchat. "Privacy Center" <https://www.snap.com/en-US/privacy/privacy-center/>
[83] Instragram. "Terms of Use" <https://help.instagram.com/478745558852511>

In line with the hypothesis of this analysis, we are therefore arguing these procedural safeguards, as seen in the case-law interpreted from the ECHR, do not fulfill the needs of the interpretation of the ICCPR under international law in context the Human Rights Committee resolution 68/167.

Furthermore, this chapter establishes the right to privacy is a fundamental and innate right, protected under international law, where although certain limits warrant the need for interception of communications, and thus potentially personal information, we hypothesize the law under the ECHR is insufficient to the standards of international human rights law. Each of these cases in the ECtHR teaches us something new about privacy in the digital age, and for this reason, the core procedural components of interception will be examined to discover the reasoning behind, the potential legality, and process under which the right to privacy is either to an extent fortified or disintegrated by the judgments, and if possible, can be applied to international law under the ICCPR.

In conclusion, when interpreting the ICCPR under the language provided by resolution 67/168 from the Human Rights Committee, in addition to the Human Rights Council on "the right to privacy in the digital age", there appears to be many similarities to the safeguards to the right to privacy as the ECHR. Using Article 8(2) of the ECHR as the foundation for the research in the next section, we will, deconstruct, so to speak, the procedures of surveillance and interception of telecommunications in cyberspace, make findings within the case-law that are sensitive to the right to privacy in the digital age as per the resolution in discussion, and finally compare whether the approach of the ECtHR would be reflected in international law and norms of the ICCPR provided with the context and interpretations listed above. It will then be concluded as to whether such a relationship can be drawn, and after doing so, determine whether the interpretations were sufficient to the protection to the right to privacy in cyberspace.

Part I, Satisfying Article 8, Section 2, European Convention on Human Rights

One of the first steps, naturally, in order to determine how a circumstance applies to the the Article is to determine whether or not that this circumstance fits into Section 1, first, and then we assess its applicability in Section 2. Firstly, "everyone has the right to respect for his private and family life, his home, and correspondence,"[84] as stated within the first Article of the Convention. Under certain conditions, as outlined in Section 2, an individual might be subject to a restriction of the interpretation of the right depending on the actions the occur within a society that could potentially inflict issues upon the human rights of others as well. In one of the first steps of a surveillance or clandestine operation, there must be "an exception to the right guaranteed by the Convention"[85] as stated in Article 8(2) of the Convention on "private life", as giving the actions of said operations a permissible legal quality. This part of the analysis essentially provides scope as to what exactly is an "exception", how such an understanding of an exception may interact with an interpretation to Article 17(2) of the ICCPR, in addition to how "exceptions" generally may be viewed in the interpretation of privacy in the digital age.

In the general interpretation of privacy or private life under these conventions and laws, there is an implicit agreement between the ICCPR and the ECHR that, to some extent, the right to privacy does indeed exist. However, it should not be taken for granted that rights, especially the right to privacy in the context of our analysis, is vulnerable to circumstances, exceptions, and scrutiny. In assessing what interference is within the scope of the ECHR it must firstly be "in accordance of the law" as stated in Article 8(2), and furthermore must be seen as to whether the contested legislation was "necessary in a democratic society", for the "prevention of disorder or crime", or perhaps "in the interests of public safety."[86] In our analysis we view this characteristics separately in order to understand the procedure to which interception, and thus surveillance, operates, if such a process can be understood this way, and how we can assess if possible is subservient to the ICCPR as per our hypothesis. In contrast, the ICCPR, under the

[84] *Supra. ECHR. Art. 8(1)*
[85] ECtHR. *Klass and Others v. Germany. no. 5029/71.* Par. 42. 6 September, 1978.
[86] Ibid. Par. 44

interpretation from the general report from the Human Rights Council[87], in addition to reference to general comment No. 27 from the Human Rights Committee on article 12 of the ICCPR[88], states "the relation between right and restrictions, between norm and *exception*, must not be reversed"[89] in further stating that the measures not only need to be permissible in that particular situation, but "must also be necessary."

Furthermore, "in accordance with the law," in our view, will be seen as the core foundation to Article 8(2) of the ECHR moving forward, followed by how "necessary in a democratic society" functions in the relationship with "the law", and then assessing as to whether or not the actions were "proportionate". Therefore, in the first step of evaluating interception and surveillance, is to see if the action was "in accordance of the law" which will stand as our focal point of this section, which after is then determined if the action was "necessary in a democratic society." Both instances will be assessed under case law on Article 8(2) of the ECHR to determine if such an interpretation meets the verbiage of the HRC report on the the right to privacy in the digital age, in addition to resolution 68/167, as it is applied to Article 17(2), and whether or not such interpretation and protections are adequate.

A.) "In accordance with the law"

The first step of the process is to determine whether the interference, regardless of being permissible under the law, is *in accordance* with the provisions, aims, and objectives of the Covenant, is *reasonable* within that circumstance, and is thus *proportionate*.[90] Therefore, the Covenant is to be interpreted in this way of the "provisions", "aims", and "objectives" whereas the ECHR comparably states the necessary requirement of being in accordance of "the law." Given the context provided in such an interpretation from the Human Rights Committee above,

[87] *Supra.* Human Rights Council, on 68/167
[88] HRC. CCPR/C/21/Rev.1/Add.9 General Comment No. 27, 1 November, 1999.
[89] *Supra.* Human Rights Council on 68/167 Par. 25.
[90] Ibid. Par. 21.

in context of resolution 68/167, we hypothesize that the interpretation of the ICCPR extends the protection of privacy with "in accordance" language more robust than the ECHR under Article 8.

In order to determine whether or not our hypothesis stands, we first view under the ECHR, "in accordance with the law" in Article 8(2), the article possesses a distinct legal interpretation for the purposes of surveillance that we are to explore, which pertains in a large part to the law of the Member-state in question; however, this is not so to say that the ICCPR stating "provisions" as noted above, is in any sense less legal in context to "with the law". Keeping in mind the introductory interpretation of the ICCPR that interference had to be in accordance of "provision", we will move forward to see if some key issues to the right to privacy "in accordance of the law" under the ECtHR case-law would appear weaker to this provided interpretation of the ICCPR.

i.) Case-law and "*in accordance with the law*"

In accordance of the law can be seen in the interpretation of the ECtHR as to whether or not the domestic law that is in question possesses adequate safeguards within the law in addition to whether such domestic law is proportionate to international law and norms as well. Additionally, I take the perspective of "legitimate aims" as explored in case law, to further demonstrate how else "in accordance of the law functions. In *Klass*, interference was conducted under the Acts furthered by the German Parliament, in the exercise of its jurisdiction, which is held by "strict conditions and procedures" of the legislation[91] further noting the widespread safeguards within the law that exists in order to protect the right to privacy. Therefore, the *Klass* case draws together a relationship between "safeguards" and "the law" which is why we believe that safeguards are an inherent characteristic to understanding part of the basis of "in accordance with the law" as the case was admissible[92] but did not find any violation to Article 8 of the Convention.[93]

[91] *Supra. Klass*. Par. 43
[92] Supra. *Klass.* Par. 26
[93] Supra. *Klass.* Pp. 28.

In accordance with the law also pays attention to the "law in question" and whether or not it is compatible with the rule of law, and as already stated, is available to the party in question.[94] Interference, thus, could have a "legal basis" for which it operates, but importantly for this case, it must also possess a "foreseeability" requirement[95] which even as referenced in *Weber and Saravia* was seen there as "strategic monitoring" rather than with the monitoring of individuals.[96] It was noted that there should not be any distinction to accessibility and clarity of surveillance per the individual or generally surveillance practices. The question exists as to whether Article 8(2) perspective of a foreseeability requirement would function under the operation of the ICCPR respective article on exceptions.

In *Klass*, in order to prevent applications for surveillance that were potentially "haphazard" there was a need to submit "due and proper consideration" under rigid administrative procedures for request of surveillance where decision can only be made by a Federal minister[97] which further shows that under interpreting Article 8 of the Convention in this context, that if there are issues within the administrative procedure, and that of applications perhaps as this has shown, then it is likely to violate Article 8 of the Convention in that "limitative conditions"[98] must be satisfied before any such operation of surveillance can take place.

Additionally, understanding what is "in accordance with the law", in addition to the inherent roles of of supervision and implementation that accompanies the law, sets an appropriate precursor for illustrating a foundation under which what is "necessary in a democratic society." In *Weber and Saravia*, assessing the provisions of the G10 Act was a part of this process to safeguard against arbitrary interference, and with this, citizens were provided with information as to the conditions of public authorities having the power to resort to surveillance

[94] ECtHR. *Liberty and Others v. The United Kingdom*. no. 58243/00 Par. 59. 1 July, 2008.
[95] Ibid. Par. 60.
[96] *Supra. Liberty and Others.* Par. 63.
[97] Supra. *Klass.* Par. 51
[98] *Supra. Klass. Par. 51.*

practices.[99] In accordance with the law, therefore, means that a citizen of that State must be able to retrieve, or have access to, the information on surveillance practices of the State publicly available in addition to the law must be clear and intelligible as was stated above.

Being in accordance with the law could be interpreted to be needing to meet the needs of international law, even in the aspect of territorial sovereignty[100], however generally, means that the impugned measure should have some basis in domestic law in its quality, accessible to the person in concern, as stated above, and must "be able to foresee its consequences for him"[101]

One measure that may be of concern to potential abusiveness is that sometimes it might not be "even feasible" to provide subsequent notifications of surveillance to individuals after an operation has been completed because it might reveal information on methods of intelligence gathering and thus the efficacy of interference altogether.[102]

In Klass, a secret surveillance order remains for three months and may only be renewed by the repeat of the application to be approved by the Federal Minister including that only an official qualified for judicial office can examine the information and either forward or destroy said information based on relevancy to the investigation.[103] Therefore, under protection of certain safeguards, implementation measures, in this case Germany, could take into consideration of what is indeed legal, but also what may be "necessary in a democratic society" which will be explored below.

Secret surveillance is only tolerable under the Convention "only in so far as strictly necessary for safeguarding the democratic institutions" and is justified only if it is in accordance with the law, pursues a legitimate aim of Article 8(2), and is necessary in a democratic society.[104]

---

[99] ECtHR. *Weber and Saravia v. Germany. no. 54934/00.* Par. 101. 10 January, 2000.
[100] Ibid. Par. 81.
[101] *Supra*. *Weber and Saravia. Par. 84.*
[102] *Klass. Par. 58*
[103] *Klass.* Par. 52
[104] *Szabo and Vissy v. Hungary.* Par. 54

Initially, the problem I has with in accordance of the law was that I thought this meant if the actions of a State, or party, were in line with "the law", interpreted as domestic law, then the actions were justified. However, given the scope of the law in the interpretation of the text was widened to the extent of international laws and norms, both expressed in the interpretations of the ICCPR and the ECHR in context of the digital age and surveillance, we can conclude that based off of these findings, there is protection "in accordance of the law" in not only the ECtHR under the ECHR but also to that of the ICCPR under the Human Rights Committee.

ii.) Under the Perspective of "Legitimate Aims"

The underlying issue behind the right to privacy can be drawn from its very definition as to the sensitivity of the subject matter. Why is it that individuals are pressing the point to the courts that there is such a problem in the first place? The need to establish that there is this innate right to privacy is shown in between what is "legitimate" versus what is "arbitrary". Not that is meant to draw a distinct binary opposition parallelism with right, wrong, legitimate, and arbitrary, but more of to show the legal extent to which privacy is and is not protected. However, although we briefly went over these concepts in the chapter exploring privacy, we will now extrapolate the idea of legitimacy and arbitrariness in context of surveillance practices in the digital age in order to highlight a certain legal character that the right to privacy is developing during this time to understand why and how actors circumvent privacy practices or why individuals feel their privacy has been circumvented.

Legitimate aims are to been viewed as the justified purposes for conducting surveillance practices of intercepting personal or telecommunication data.[105] What is just, however, can range on the extent to which such protections exist under domestic law as it can be seen that some nations have a clearer understanding of their legitimate aims than others. Russia, for example, possesses the, at the time, Operational Search Activities Act (OSAA) which essentially uses operational-search to legitimate surveillance to include the detection, suppression, and investigation of criminal offenses in addition to tracing fugitives or preventing crimes against the

[105] Include source on a legitimate aim

Russian Federation.[106] This happened to be the case in *Roman Zakharov v. Russia*[107] where the legitimate aims of interception had to have met "reasonable likelihood", in the perspective of Russia, with the exceptions presented above, in order to even submit an application against the violation of article 8 to the convention. However, in international law, "legitimate aims"[108] for surveillance must be met with Article 8 paragraph two of the convention of what "is necessary in a democratic society"[109] which can include "protection of national security, the prevention of crime and the protection of well-being of the country."[110] Furthermore, what is found to be "necessary in a democratic society", and thus legitimates such aims, is subject to the unique situation of the case and the domestic institution must possess "effective guarantees" against abuse of secret surveillance.[111] This language is perhaps worded in such a way that guarantees the objectivity in approaching legitimate secret surveillance per each case which is perhaps the reason the European Court of Human Rights approaches a "necessity test"[112] balanced with "in accordance of the law"[113]. Therefore, the European Convention is examined for proportionality with the domestic legislation for guarantees against abuse, like in *Kennedy* cited above, and after such a procedure, legitimacy for conducting secret surveillance is potentially fulfilled in European Law. Nevertheless, it appears that surveillance is generally accepted as a normal activity of the State under certain circumstances despite the implications on privacy rights.

However, the important aspect of the matter of privacy in context of the digital age is whether or not that information, and thus that individual, is a victim of abusive practice of surveillance. Although this may not be necessary by the actions of the State, for the purpose of our study, we will take a look at under how abusive practice is approached in case-law in order to understand under what conditions a state actor has gone too far for violating its citizens, and perhaps the citizens of other states rights- as will be explore more in the latter chapter on extraterritorial surveillance.

---

[106] OSAA Section 8(2). Russia. 12 August, 1995.
[107] ECtHR. *Roman Zakharov v. Russia.* no. 47143/06. Section 154. 4 December, 2015.
[108] Ibid. Par. 227.
[109] *Supra.* ECHR Art. 8 Par. 2.
[110] *Supra. Kennedy.* Par.155
[111] *Ibid.* Par. 153
[112] ECtHR. *Kvasnica v. Slovakia* no. 72094/01 Par. 80. 9 June, 2009.
[113] *Supra*. *Kennedy.* Par. 155.

iii.) Concluding remark

In conclusion, we see no difference between the usage of "in accordance of the law" or "previsions" stated in the interpretation of the ICCPR in the digital age, and therefore conclude the ICCPR in the Human Rights Committee would merit no, or trivial, differentiation in interpretation of this notion of "in accordance" should the ECHR interpretation apply to the HRC. Therefore, our hypothesis does not stand due to such similarities in interpretation of "in accordance" of either law or provisions, in especially how such an interpretation was applied to the ECtHR case law. It is therefore believed that had the HRC be provided with similar cases, they would apply the principals of "in accordance of the law" as the ECtHR did in a very similar method to the extent provided by both the ECHR and ICCPR regardless if such an extent merits growth to deeper protections.

In perspective of such a conclusion though, we ask ourselves that regardless if this occurs to be a very much parallel interpretation, between both the ECHR and the ICCPR is this sufficient to address the right to privacy in the digital age? Is there a weak-link, as was stated in the introduction, within this interpretation of the respective Convention and Covenant? I believe that, although that the ECHR can be interpreted to the protections inherent within the ICCPR, that this is potentially not enough for protecting privacy in context of telecommunications surveillance. As was seen in the case law, and stated throughout this section, since we believe the HRC would rule no differently given the parallel legal language, we can presume that the ECHR under international law would possess very similar shortcomings as was listed in the issues with the case-law explored above. Some of the common issues that were analyzed throughout included whether the domestic law in question was proportionate to the value stipulated within the Convention. We see as the ECHR does have shortcomings in this sections, we believe that the same shortcomings would become apparent under similar case-law in the HRC, and thus in conclusion the right to privacy under international law possesses shortcomings in these areas.

B.) "Necessary in a Democratic Society"

Nevertheless, the Human Rights Council has illustrated that individuals are entitled to an effective remedy under Article 2(3) of the ICCPR governed by judicial oversight and what is "permissible in a democratic society"[114] However, this of course depends on to what extend we interpret permissibility and it is the circumstances of such an interpretation that matters for the protection of our privacy.

i.) "The Necessity Requirement"

In light of the wide scope of potential avenues of telecommunications interception, it could be argued that in the digital age the interpretation of what is necessary is used in such a generous way. As was beginning to be stated earlier, "the necessity requirement" provides that perhaps just because interference might be legal, and might be legitimate, does not guarantee that such compliance is in line with the conditions of Article 8 of the ECHR.[115] This aspect is argued to be responsible for the "collision between the individual and society" and in order to determine this requirement, such a "proportionality test" extends scrutiny, to the right to privacy in our case, by viewing the democratic character of the interference in using indicators such as "pluralism, tolerance, broadmindedness, equality, liberty, right to fair trial, freedom of expression, assembly, and religion."[116] Conducting such a test to determine whether the surveillance is proportional under the ECHR is to be more understood as a byproduct of what is necessary rather than interpreting them as separate entities of each other. Given the interwoven roles of proportionality and necessity, necessity is generally defined as a "composite and balanced" notion in addition to the important variable of "the passage of time" determining continuity of necessity.[117]

---

[114] *Supra.* Human Rights Council. "Right to Privacy in the Digital Age" Par. 41
[115] Roagna, Ivana. "Protecting the right to respect for private and family life under the European Convention on Human Rights" *Council of Europe Human Rights Handbooks.* Pp. 44. Strasbourg, 2012. Web.
[116] Ibid. Pp. 44.
[117] *Supra.* Roagna, Ivana. Pp. 44.

The Human Rights Council, on the other hand, in context of also the Human Rights Committee (HRC) on resolution 68/167, also recognizes that "surveillance of electronic communications data can be necessary"[118] for intelligence gathering or law enforcement. Additionally, the HRC notes interference must be "proportional" and "necessary" in the circumstances of the case[119] by drawing comparison to *Toonan v. Australia*[120] without context to telecommunications surveillance; however, drawing to "necessity" as general principle. Under the HRC, and thus the ICCPR, it must also be as least intrusive as possible[121] and it may be necessary in intelligence gathering for the prevention of crime and terrorism.[122]

Moreover, necessity plays a vital role in our assessment of the right to privacy as it applies to cyberspace and will be an inherent part in exploring the process of interception in addition to interception in the context of extraterritorial surveillance. The necessity requirement is something that, in the above defining characteristics as defined for the ECHR, may be perhaps perceived differently under the ICCPR considering the ICCPR does not have language at all on necessity in the direct text of the article. One could perhaps argue that this necessity is an implicit character of the ICCPR as the language states that there will be no "arbitrary" or "unlawful" interference; however, this does not necessarily warrant the use of non-arbitrary or legal interference as well. Moreover, the language of the ICCPR is general to the character of how privacy should not be approached and leaves indirect definition of circumstances under which such a right is interpreted. Given the wide application of Article 8 of the ECHR in the ECtHR, under the purposes of "prevention of disorder or crime" in addition to the "interest of national security" in case law, we could potentially presume cases that are inadmissible to such a violation in this perspective, are fulfilling the necessity requirement as described above in addition to being proportionate. Nevertheless, as described, because of the even wider scope of the ICCPR interpretation of Article 17(2), perhaps more cases would be determined admissible in the Human Rights Committee under a different interpretation of what is necessary.

[118] *Supra*. HRC. 27/37. Par. 15.
[119] *Supra.* HRC. 27/37. Par. 21.
[120] HRC. *Toonan v. Australia*. CCPR/C/50/D/488/1992. Appendix. Par. 1.
[121] *Supra*. HRC. 27/37. Par 23.
[122] Supra. HRC. 27/37. Par. 24.

Therefore, the right to privacy in an absolutist perspective, could be argued would never truly be upheld, due to the fact that international law, in addition to laws and norms presented within the ECHR, in addition to many of the domestic legal frameworks on privacy perhaps based off such international laws, provide a certain extent to the interpretation of the right in order to safeguard the rights of others in a democratic society as utilizing an interpretation of what is "necessary" to circumvent the right to privacy. Which, altogether, is an interpretation that has basis within the context of the the right to privacy in the "digital" age as shown above and in conclusion we believe that the right to privacy not only has presence in the digital age, but such a presence is inherent within the original meaning of the right to privacy and is expressed by providing a deeper interpretation of the legal process to "interception" in the ECHR or preventing "arbitrary" action under the ICCPR.

ii.) Case-law

In *Klass and Others v. Germany* there was a need to discover whether Article 8(2) of the Convention justified interference in the form of secret surveillance which the court argued is "tolerable" as much as that it is "necessary for safeguarding the democratic institutions."[123] However, not all instances that are "in accordance with the law", as described above, may necessarily be "necessary in a democratic society" which is why separating these characteristics of Article 8(2) will deepen an understanding to the language in which it is applied. What is potentially included to the conversation as necessary is perhaps legislation that grants secret surveillance of telecommunications as a result of the heightened development of terrorism in Europe in recent years and thus the need for sophisticated forms of espionage to acclimate or counter such threats.[124]

In *Klass*, it is noted that since the individual is not aware of the secret surveillance operation being undergone, that the individual's rights are safeguarded in this process, while at the same time the supervisory procedures follow within the meaning of Article 8(2).[125] The court

[123] *Supra. Klass.* Par. 42.
[124] *Klass.* Par. 48
[125] *Klass.* Par. 55

views that in order to avoid abuse to the fullest extent supervisory control should be entrusted to a judge; however this can also be interpreted in the sense of an independent authority, separate to the authority conducting the surveillance, with sufficient powers of control.[126]

In comparing how both Article 8(2) of the ECHR and Article 17(2) of the ICCPR as to how what I justified as a measure necessary in a democratic society could aid in the scope of privacy's application to cyberspace. Compromise between the requirements for defending democratic society and individual right is argued as inherent in the system of the Convention which in context of Article 8, is that there must be a balance between the right guaranteed to that individual in the first article and thus the necessity of the secret surveillance as another issue in the second article[127]. In contrast, the ICCPR could interpret this as…

C.) **Abusiveness** and Arbitrariness affecting the right to privacy

In order to understand the parameters of where this is coming from, further context on the right to privacy in the digital age was given from the Human Rights Council under the request from the Human Rights Committee on resolution 68/167. The Human Rights Council defines the terms "unlawful" and "arbitrary interference", in context of the right to privacy, in response to the general output of states, at the time, had insufficient legislative protections for the article.[128] "Unlawful" being that the only permissible interference had to comply with the law, or objectives, of the covenant while "arbitrary interference", with intervention with the law, should be reasonable for the particular circumstances. Furthermore, the context under which "interference" was established and founded upon called for a transparent legislative processes under which such interference was permissible in addition to detailed records of filed complaints on violations of article 17.[129] In interference, the integrity and confidentiality of the correspondence should be delivered without interception "and without being opened or otherwise

[126] *Klass*. Par. 56
[127] *Klass*. Par. 59
[128] *Supra.* Human Rights Council Report. Sec. 2.
[129] *Supra.* Human Rights Council Report. Sec. 6.

read."[130] As will be seen, this is not always the case, by both state actors and third-party actors, involved in telecommunications, which has fundamental implications for the protection of privacy rights in the digital age. Privacy relies on the prevention of arbitrariness and abuse when personal data is available under certain protocols, like that especially for reasons of "national security" as directives of the EU have noted.[131] By examining where privacy of individuals has been inflicted upon negatively in key case-law, perhaps we can see where the issues with legislative output has occurred and we can examine any common reoccurrences, or any problems, despite the detailed European legislation on approaching the right to privacy and the right to personal data as a result. Abusive or arbitrary actions of surveillance will therefore be stratified into additional categories of understanding: through the minimum safeguards, or lack thereof, in question, the nature of the offense in question as to whether the action was indeed arbitrary, the length of time the surveillance was conducted for, and the procedural collection and storage of the data.

i.) Arbitrary Surveillance due to lack of Safeguards

The risk to privacy in the digital age could be as a result of inadequate safeguards put in place by governments that oversees the procedure of clandestine intelligence-gathering or surveillance to prevent an arbitrariness or abuse. Safeguards, in this view should be separate to the understanding of "in accordance of the law", "necessary in a democratic society" and "the necessity requirement" as it is more of a function within the law and interpretations of the legal documents put in place in order to prevent abuse of those aims in the first place. Safeguards are potentially the risk factor to privacy in cyberspace because some governments may have greater measures to protect these rights than others. The issue stands that though nations have responsibilities of protecting these rights of individual's personal data, and thus their privacy, without safeguards in even some nations still poses a risk for individuals who reside in other nations that do possess such protections. Although later we will explore extraterritorial application of safeguards, this section takes into account generally some of the issues that may exist with arbitrariness and safeguards in surveillance operations.

[130] *Supra.* Human Rights Council Report. Sec. 8.
[131] Insert supra note from the EU directives above.

To prevent the arbitrary or abusive act of collecting of personal data in a way the infringes upon individual's privacy rights, it is essential that a nation possess adequate safeguards in order to ensure that all actions are indeed legitimate to the investigation. Altogether, interception of communications has a qualitative requirement when being authorized meaning that it must meet "in accordance with the law" having basis not only in domestic law but is also compatible with the rule of law inherent to the object and purpose of article 8[132] while must meeting the minimum safeguards in order to avoid abuse or arbitrary use of power which could even include duration of telephone tapping and storage of data.[133]

Principally, in the *Zakharov* case, Russian domestic law did not possess the adequate safeguards against arbitrariness and permitted automatic storage of relevant data which also did not comply with the above described requirements "necessary in a democratic society."[134] This interpretation, although vague, gives the ECtHR the power to take each violation to private life as a unique case; however, this does not take away from the fact that states, such as Russia, in this case that occurred last year, and which is assumed being fully aware of the conventions, directive, norms, and protocols explored in the above chapter on the legal framework on privacy, are still committing crimes against individual's right to privacy. Indeed, this shows that the court does take the nature of the situation in order to address the safeguards, because in defining arbitrary above, the court must assess if the interception was reasonable for particular situation. This begs the question of whether there are issues with accountability, implementation issues, or authority issues at the domestic levels. However, this mundane process of determining whether the actions of states are arbitrary could be perhaps due to lack of legislation that holds states accountable for lack of safeguards in the first place. In the *Zakahrov* case, the arbitrariness included the lack of safeguards with the supervision of the personal data; moreover, that the personal data was vulnerable without being under the oversight of a court and that without such oversight, the vulnerabilities included the ability of state authorities to easily be able to conduct surveillance without a court order. Alternatively, in *Uzun v. Germany* the necessary safeguards

[132] *Supra. Zakhavrov.* Sec. 228
[133] *Supra. Zakharov.* Sec. *231*
[134] *Supra*. *Zakharov.* Sec. 302.

from the "Code of Criminal Procedure" in Germany's domestic law were in place prevent the individual's total arbitrary GPS surveillance and the court concluded its sufficiency and proportionality against abuse.[135] In this case, while there was reason for the individual to have his surveillance conducted upon, the case was declared there was no violation of Article 8 of the Convention. Therefore, there was legitimate reason for the government to surpass the individuals right of privacy and collect information as they found sound for investigation and potential criminal proceedings. Safeguards are indeed an aspect that is important to the right of privacy in the digital age, because as we can see in these two cases, there is just reason to lose one's right to private life in Article 8 of the ECHR via surveillance if the intentions are for potential criminal proceedings and the safeguards to protect the individual's personal data was sufficient enough in the eyes of the court.

In *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* the principal issue within the case was that there were lack of safeguards from the constitutional court under the Special Surveillance Means Act (SSMA) of 1997 as "at any point in time without any notification to, during, or after" that individuals could be subjected interference of their personal data.[136] The court found that although the initial stages of "authorization" of surveillance under SSMA might, as a stretch, possess substantial safeguards,[137] it determined that Bulgarian law didn't sufficiently provide enough guarantees to prevent abuse of secret surveillance and thus found violation of Article 8 of the Convention.[138] What can be understood here additionally is that even though one part of the domestic law may seem to safeguard the privacy rights of individuals for surveillance, all stages of the procedure of clandestine operations must meet requirements or therefore personal data is vulnerable to abuse.

Similarly, using the foundational safeguards against abuse from *Weber and Saravia,* cited above, the court in *Kennedy* assessed if the United Kingdom possessed adequate safeguards

[135] *Uzun v. Germany*. Sec. 73.
[136] ECtHR. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria.* No. 62540/00. Sec. 6. 28 June, 2007.
[137] Ibid. Sec. 84.
[138] *Supra. Ekimdzhiev.* Sec. 93.

under the RIPA regime.[139] Although the United Kingdom in this case has less of international and regional compliance issues than Russia did on adequate safeguards, the principal observation is that both cases assess what is necessary for a democratic society using their respective regulations or regimes and determining their compliance with the articles of the convention. Therefore, the court is making a point in indeed taking each particular case unique to the situation in approaching privacy; however, they are fundamentally trying to point out the fallacies in domestic legislation not recognizing the necessity also recognizing international protocol on data collection that abuse of power on the right to privacy might exist and where they must rectify language in order to prevent issues in the future.

ii.) Supervision necessary for adequate safeguards to privacy

In the *Klass* case the basis of the supervisory powers was determined to be sufficient safeguards and even that the "exclusion of judicial control" did not "exceed the limits of what may be deemed necessary in a democratic society."[140] This shows that, in contrast to the *Ekimdzhiev* case as was explored above with authorization as one of the steps of safeguarding against abuse, the courts found in this situation that have at least supervisory powers of the situation was sufficient safeguards even though one may argue that all steps of implantation of necessary legislation for full safeguards were not fulfilled. This situation with *Klass* took into consideration of the "competent Minister" in the *Bundestag* responsibility for continuous and effective control of clandestine surveillance operations. However, it was further noted by the court that a judicial authority does not necessarily need be the authority under the implementation of "concrete surveillance measures"[141] and in addition that, given understanding that the authority was the G10 and not a judicial authority submitting the surveillance operation, there was no violation of Article 8 of the convention.[142] The *Bundesnachrichtendienst* possesses the G10 commission as a body that monitors the processing, collecting, and utilizing of personal

[139] *Supra. Kennedy*. Sec. 158.
[140] *Klass.* Sec. 56
[141] Ibid. Sec. 67
[142] *Supra*. *Klass.* Sec. *75.*

data in surveillance under Article 10 of the German Constitution.[143] The G10 commission, though of course entirely different in function, is similar to the ECtHR interpreting a case under Article 8, in the sense that in Germany the G10 decides on "the legitimacy and necessary measures which restrict the privacy of correspondence."[144] Additionally, the G10 is appointed by the *Bundesamt für Verfassungsschutz* (BfV) for a single term of the German *Bundestag* which is chaired by an individual qualified to hold judicial office.[145] In the *Zakaharov* case it is further demonstrated that having independence from a judicial authority is absolutely necessary in order to safeguard against abuse from authority.[146] Therefore, in *Klass* the G10 Commission possessed safeguards against abuse that put "surveillance measures to an unavoidable minimum" and ensured that it complied with the law regardless of its lack of standing as a judicial authority that should or should not authorize the surveillance operations.[147]

In terms of supervision in context of abuse or arbitrariness, the court has also noted how easy abuse is from a state and that it is necessary to establishing supervisory control to a judge in order to maintain order of these privacy protections.[148] When a judge was established as the supervisory authority to the conduct of surveillance, and the material protected under a court's jurisdiction, the chances of abuse of power in the eyes of the court are lesser. Additionally, This is understood without having adequate supervision or clear language in law, it may not comply with the necessary effective and continuous control effecting operational organization of surveillance.[149] In contrast monitoring provisions should be counterbalances with reasonable limitation of the offenses

As far as implementation is concern in relationship to supervisory powers, "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner

---

[143] *Bundesnachrichtendienst.* G10 Commission. http://www.bnd.bund.de/EN/Scope_of_Work/Supervision_and_Control/G10_Commission/G10_Commission_node.html
[144] *Bundesamt für Verfassungsschutz*. "Parliamentary Control" Par. 9.
[145] *Ibid. Bundesamt für Verfassungsschutz.* Par. 8.
[146] *Supra. Zakharov*. Par. 292.
[147] *Supra. Klass.* Sec. 59.
[148] *Supra. Kennedy*. Sec. 161.
[149] *Supra. Zakharov.* Sec. 303.

of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."[150]

iii.) Safeguards to Prevent Abuse of Length of Time of Surveillance

The length of time that surveillance is conducted for is a matter that indeed can have implications on the privacy rights of the individual because of the risk of surveying without any adequate reason and therefore collecting personal data that may not even be disposed or handled proper under the same violating authority. What is exactly an adequate length of time? What is the right amount of data that can be taken? Moreover, what verifiable measures in the law can be found that an "abuse of power" has actually occurred? The court rules that although states possess the inherent power to determine what is necessary in a "democratic society" that the state is subject to the law within the court in order to uphold these protections.[151]. Therefore, abuse of power will be examined in that it approaches surveillance in a way where states, or involved actors, should be fully aware of the law on data collection and surveillance given the scope of data protection in European courts has existed for over thirty years and it is partially for this reason that states are expected to not only prevent abuse, but to have implemented measures within their domestic legislation to avoid any such issue being brought to the courts on the matter.

Cases brought to the court, however, may not only be the only issues occurring with privacy, so additional accountability measures in the prevention of abuse appears to be a legislative deficit in the protection of privacy- and that especially in the digital age given the large amounts of data. Mass data collection, in particular, is an abuse of power that cannot be ignored in context of the digital age, and it is this that will be explored in the next section but as a sub-category of a larger chapter addressing extra-territorial application of the protection of human rights- but of course more specifically, the privacy of data.

D.) The role of personal data

[150] *Supra*. *Zakharov*. Sec. 230.
[151] *Supra. Zakharov*, Somewhere around 240

Although each situation falls under a particular circumstance[152], there is no clear indication of what is the right amount of data that can be taken, for how long, and how the data should be treated. Personal data is potentially argued as paralleled with one's privacy and thus their right to privacy, which is why this next section explores the role data plays in the right to privacy in the digital age and why its intricate legal components matter as to whether protection of this right is upheld.

Additionally, interference also needs to consider the aspect of the transference of data and what this could potentially mean for the rights of individuals. In some instances, the transference of data could meet the "reasonable limitation of the offences" with the "supervisory mechanisms against abuse"[153] however, this highlights the counterfactual of this idea of the potential vulnerability that data exists as. Personal data could be transferred between authorities without the necessary cause and it is this factor that is troubling to maintaining the right to privacy of the individual- especially when the said operation is under the protection of the State's requirement of secrecy for clandestine operations of the sort. The interpretation of data, under the ECHR and the ICCPR, was stated more so in the key terms chapter, however, they both possess shortcoming to protections that are not potentially inadequate to a strong interpretation of data protection- as was shown in the vulnerabilities and circumstances with the case-law.

[152] *Klass and Others v. United Kingdom*
[153] *Supra. Weber and Saravia.* Par. 129.

VI, Privacy and Extraterritorial Surveillance

The staple of surveillance analysis veers to the Snowden revelations of mass drag-netting of personal information that in essence violates not only arguably violates the fourth amendment rights of United States citizens, but also that of international human rights law and norms. When analyzing international human rights law, we find that in the analysis of privacy in the digital age that for the most part there is no general distinction of rights that a citizen in one nation should be privileged to possess over a citizen of another nation for the same actions.

In more fundamental than simply jurisdiction is the sensitivity of actions of treating human rights fairly across the globe; however, we did find in the analysis that, under certain legitimate, and legally proportionate, circumstances, that certain cases were justified to the loss of privacy for criminal investigatory, or for the protection of public and national security, purposes. Therefore, the extent to which privacy is protected in the digital age, could not only depend on the actions of the state but also the actions of the individual, but moreover at this stage we are going to explore when those actions are taken in the aspect of territory. This has been a subject avoided up until this point because understanding the general procedure of surveillance of personal information seemed to be a necessary foundation prior to this conversation.

A.) How jurisdiction operates in International Frameworks

If an individual, or actor is within the jurisdiction of a state, as we also explored above on interpretation of jurisdiction of the ICCPR, that should not necessarily entail that the individual or actor is a national or citizen of that nation;[154] however, this should not necessarily mean that because the drafters of the ICCPR did not include *extraterritorial* usage of privacy rights, or extraterritorial usage to human rights and freedoms altogether, that it should or could be eliminated from the discussion. Just to reiterate from the international legal framework chapter, Article 2(1) of the ICCPR is the basis for the upcoming analysis in order to discover the understanding of extraterritorial surveillance on the individual. This article of the ICCPR states:

[154] *Supra.* Milanovic. Pp. 99.

*"Each State Party to the present Covenant undertakes **to respect** and **ensure** to all individuals within its **territory** and subject to its **jurisdiction** the rights recognized in the present covenant."*[155]

In comparison, Article 1 of the European Convention of Human Rights states:

*"The High Contracting Parties shall **secure** to everyone within their **jurisdiction** the rights and freedoms defined in Section I of this Convention."*[156]

Although the language of the ECHR does not present a descriptive scope of territorial aspects to these rights, the question here still stands as to whether this vague description can still hinder the protection of privacy in cyberspace. Is the flawed language the only impediment to the protection of privacy only and especially to the collection of personal data in mass-form, or even extraterritorially? Additionally, the ICCPR also does not provide us with the necessary language to apply to extraterritorial surveillance either which also is a point of interpretative concern in the pending analysis on the subject. Given that throughout case-law that we are exploring through the Human Rights Committee, the Court of Justice of the European Union, and the European Court of Human rights, that there is no specific case on extraterritorial *surveillance*, the cases that we do explore are on a matter of extraterritorial argumentation to rights generally so that we can apply these models under interpretations of privacy in the ECHR and the ICCPR while continuing to understand their interpretation of territory and jurisdiction as well.

Although this analysis does not use the United States as an empirical and core component to this analysis, the approach of discourse on surveillance here will provide a perspective of the United States involvement in mass-data collection so that it can demonstrate the existential risk the right to privacy in the digital age possesses because of this type of action. More importantly, it provides a precursor to applied case-law in the Court of Justice in the European Union

[155] *Supra.* ICCPR, Art. 2(1).
[156] *Supra.* ECHR. Art. 1.

B.) Territory and the collection of data

The Court of Justice of the European Union possesses two landmark cases that exemplifies some of the international legal activity on surveillance as it pertains to arbitrary collection of personal information in mass scale and provides scope to the degree of the right to privacy in an age of virtual surveillance. These cases highlight some of the fundamental issues with privacy rights as something that sometimes even individuals may not know enough information about regarding their own rights to privacy in addition to the potential roles of other third party actors have in the process of protecting and safeguarding privacy in cyberspace. Furthermore, given the role that search engines like Yahoo and Google possess in this digital age, and the potential information that they retain on the individual, they are an actor that should be reckoned with and understood as it not only applies to collection of data in mass generally, but how an internationalized search engine has powers that may or may not circumvent privacy laws globally while potentially being protected by laws in nations globally that have safeguards against abuse as will be explored below. This case provides context to a layer of extraterritorial surveillance that has deeper meaning and will be necessary to explore under the discretion of international law in the future.

When data is collected from an individual, it could be expected that their information was taken knowingly, as they may have provided permission in some manner; however, other times, this may not be the case, and furthermore, more information than they would have desired was taken as a result of a potentially arbitrary action. In the case *Google Spain v. Spain,* a landmark case introduced a layer to international privacy human rights law that recognizes third party's, such as news sources, have relationships with search engines that in the eyes as some may prove to be detrimental to one's right to dignity and privacy.[157] At the time, Directive 95/46, which as was explored in the chapter on the legal framework of privacy, played a significant legal role in determining whether Google collected the information legally, in addition to the established context that the Spanish government also transposed the directive into national law.[158] Moreover, this case presents a multi-pronged issue that relates to the protection of privacy that must be

[157] *Supra. Google Spain.* Par. 17.
[158] Ibid. Par. 13.

understood; the territoriality aspect, the involvement of actors as facilitators and data retainers of information, and the relationship of responsibility that this involved. Article 28 of Directive 95/46, as was said was enacted prior to the current Directive 2006, states that Member States must have a public authority within its territory to monitor the provisions within the Directive.[159] As a side note, Directive 2006/24/EC possesses less language on the role of the "Supervisory Authority" under Article 9[160] which is something left for interpretation of whether or not this aids in the protection of personal data further or is legislation that could potentially lead to greater arbitrariness in the future. Nevertheless, the activity of the supervisory authority article within the current case

Having established this potential conflict with Article 9, there arises issues that provisions under Directive 95/46 presents to the territoriality of protecting personal data. Although application of this law in this case does not specifically address extraterritorial, it still remains an important aspect of perhaps how one approaches personal information when approaching an issue with territory generally since there are borders of virtual nonexistence in cyberspace. Though this stands as a broad argument, Google Inc. establishes a sense of territoriality to the actions of personal protection in this case, which may have appears for awhile that drawing links to cyberspace and territory were not of a possibility. The search results of a page, in this case, displaying personal information of an individual that they felt harms their personal dignity, is also accompanied by commercial and advertising activity of the "controller"[161], specifically tailored to individuals within this territory, which in this case is Spain, and thus because of the legal accountability of Google on the processing of personal data, they should be held to the "obligations and guarantees laid down in Directive 95/46"[162] which includes assessing whether data subjects "has a right" for their personal information "no longer be linked to his name" which may override the interests of the general public and the economic interests of the provider if the information.[163] With search results being tailored to the particular location, or branch, of the controller, there could be reason that individuals are more vulnerable

[159] *Supra*. *Google Spain*. Par. 12
[160] *Supra*. 2006/24/EC. Art. 9.
[161] *Supra*. *Google Spain.* Par. 57.
[162] *Supra. Google Spain.* Par. 58.
[163] *Supra. Google Spain.* Par. 100. Sec. 4.

to their personal information affecting their personal life and dignity depending on the scope and magnitude of the issue that is being discusses.

In further discussion of the role of search engines, given their global scope, relevant to the retention of personal information, the view of this matter in perspective of the United States protection of privacy provides a layer to the approach of the protection of availability of personal information regardless if we are discussing Spain, the United States, or another country. The territory of which we are discussing is of importance, but drawing comparisons to similar situations perhaps will aid in discovering an approach to the fundamental issues with privacy not just within the territorial scape, but to overall privacy. In the U.S., for example, the state can obtain information from search engine logs from service providers "without a warrant" due to the "terms of use" agreement rendering information as non-private[164] of which information could even be stored for up to eighteen months before disassociating the data from the user and computer[165]. This, in relevancy to the *Google Spain* case, shows that in addition to this potentially controversial understanding of the "right to be forgotten" that in addition to search engines structuring information under a certain jurisdiction in a certain way, and letting information be available under the search engine that might be personal information in the first place, there is this layer of understanding that Google also takes information from searches, which may include but is not limited to the personal information of the individual in discussion of that search. What is important to understand about the approach to territory on the matter is that Spain had their own provisions under which Google's subdivision in Spain operates on the processing of personal data just as the United States operates on their own. Aside from what should, or could be, protections under the Fourth Amendment of the U.S.[166], the Stored Communications Act distinguishes between "content" and "non-content" data, where although content information is what would be considered more sensitive information, non-content data, including phone numbers, names, and addresses, are not afforded as many protections in the U.S. law that many would subjectively expect.[167]

---

[164] Kurt Young, Jr. "Privacy Law in the Digital Age: Establishing Privacy Rights in Search Engine Logs". *Connecticut Public Interest Law Journal*. Vol. 14, No. 1. Pp. 157.
[165] Ibid. Pp. 158
[166] 4th Amendment
[167] *Supra*. Kurt Young. Pp. 164

C.) Extraterritorial Surveillance as a Fundamental Privacy Rights Issue

Extraterritorial surveillance as a phenomenon within human rights is a matter that is continuously changing under interpretation of international law given the advancements in technology and thus partially the demand for resolutions like the UNGA resolution 68/167 addressing that it is "deeply concerned at the negative impact that surveillance and/or interception of communications, *including extraterritorial surveillance* and/or *interception* of *communications.*[168] The ICCPR operates under a foundation of laws, principles, and norms within international human rights law and, in comparison and relationship with our hypothesis, we believe that the ECHR is not sufficient, in the context of this chapter on extraterritorial surveillance, to the protections to the right of privacy in the digital age. In examining this further, the author first presents a legal framework under which extraterritorial surveillance operates under the ICCPR, followed by application of case-law to the issues observed within privacy and extraterritorial surveillance, to be concluded by a remark as to whether the aforementioned information fulfills our hypothesis on the matter.

i.) International Legal Framework; Extraterritorial Surveillance

Furthermore, the right to privacy in the digital age has undergone evolution of interpretation of international law in the Human Rights Committee regarding the ICCPR via jurisprudence of the International Court of Justice (ICJ)[169] which, although a judicial system avoided being discussed throughout our analysis, is nevertheless important for the context of international law on this subject of extraterritorial application as the ICJ supports the notion that the ICCPR can be used to interpret "exercise of jurisdiction outside of its own territory"[170] by additionally referring to the Vienna Convention on the Law of Treaties(VCLT)[171], within

[168] *Supra.* Res. 68/167. Par. 8.
[169] International Court of Justice. "Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory." General List No. 131 Par.107-111. 9 July, 2004.
[170] Ibid.
[171] United Nations, *Vienna Convention on the Law of Treaties*, Articles 31 and 32. 23 May 1969, United Nations, Treaty Series, vol. 1155, p. 331

Articles 31 and 32. Furthermore, although not to dismiss the information just stated above, the most important Article for the purpose of our study which encapsulates the aforementioned information of these legal instruments is that of Article 2 Section 1 of the ICCPR. Article 2(1) of the ICCPR states:

"Each State Party to the present Covenant undertakes ***to respect and to ensure*** *to all individuals within its* ***territory*** *and* ***subject to its jurisdiction*** *the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status*."[172]

In General Comment No. 31 from the Human Rights Committee, States are required under Article 2(1) of the ICCPR, to only undertake "measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights"[173] in addition to that a State Party is to ensure Covenant rights to *all* individuals within their territory including individuals outside of their territory or jurisdiction that are within the effective control of the State.[174]

Furthermore, we agree with the Human Rights Council that, based off the Human Rights Committee understanding, that the right to privacy comply with legality, proportionality, and necessity regardless of nationality[175] that in addition to Article 2(1) and Article 17 of the ICCPR, it is also necessary to interpret Article 26 of the ICCPR together with the former two articles in context of extraterritorial surveillance.[176] The reasoning for this agreement is because Article 26 of the ICCPR states:

"All persons are equal before the law and are entitled ***without any discrimination*** *to the equal protection of the law. In this respect, the law shall prohibit any discrimination and* ***guarantee to all persons equal and effective protection*** *against discrimination on any ground*

[172] *Supra*. ICCPR. Art. 2(1).
[173] HRC. CCPR/C/21/Rev.1/Add.13 General Comment No. 31. Par. 6.
[174] Ibid. Par. 10.
[175] Human Rights Committee. CCPR /C/USA/CO/4, para. 22.
[176] *Supra*. Human Rights Council. Par. 36.

such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."[177]

Furthermore, due to objects of discriminations and guarantees to all persons, it is potentially necessary to include, in relationship with Article 2(1), that under the ICCPR, individuals are protected and guaranteed rights in "equal protection" to that of the State's own nationals under Article 26, and that additionally, if their privacy was violated under Article 17 of the Convention due to extraterritorial practice via "unlawful interference with his privacy"[178], such interference does not have association of nationality with protection of the law and thus regardless of where an individual is located, the Human Rights Committee under the ICCPR would potentially defend the privacy rights of the individual transcends borders fluidly.

ii.) Case law on Extraterritorial Surveillance in the ECtHR

Although extraterritorial application of surveillance under the protection of privacy in the digital age has never been explored in the ECtHR or the CJEU per se, the author does not believe that it will limit the function of viewing how this phenomenon would operate under the ICCPR, and we can still draw distinctions from other human rights cases that perhaps did not base the case necessarily around privacy; however, taking a step back to view the general scope of extraterritorial surveillance or clandestine operations, in addition to the framework just presented, we will explore relevant case-law to examine how the right to privacy interacts with extraterritorial surveillance under the ECHR in the ECtHR. After drawing the relevant information from the cases, the hypothesis of this analysis will be taken again in to consideration in context of extraterritorial surveillance as to, provided the international legal framework on extraterritorial surveillance, presume the ECHR does not fulfill the scope of privacy necessary in the digital age to the extent that the right is protected under the respective Articles under the ICCPR.

When taking the basics of the idea, as implied in the definition of "extraterritorial", an individual could believe that their rights have been, or could be, violated outside of the territory

[177] *Supra.* ICCPR. Art. 26.
[178] *Supra.* ICCPR. Art. 17(1)

in question- perhaps to a neighboring state or beyond. In *Soering v. the United Kingdom*, we do not want to make any bold assumptions based on a case that had a background completely different on the right to privacy and a reputation on its extraterritorial ruling on extradition. However, given the case's reputation and scope of a state's actions on its own territory to produce an effect in another state, perhaps we can theoretically draw from the case to establish a rights-based argument rather than simply "privacy" under Article 8 versus, well in this case, "inhuman and degrading treatment" under Article 3[179] of the ECHR. Clearly these are approaching two very different human rights issues, and arguably, inhuman and degrading treatment could be common knowledge as perhaps more important, and more of a priority, to issues of privacy protections, and given the nature of the circumstances, the court's assessment perhaps cannot be viewed in such a parallelism between these two articles of rights under the convention. However, aside from the sensitivity of the issues and assumptions within this case as an example, and perhaps the cases later to discuss, strictly speaking we will be paying attention beyond the scope of acknowledged sensitivity of the rights issues presented, but will use the cases interpretations of territory for further understanding of how this potentially could function under privacy rights issues.

The *Soering* case illuminates the interpretation of the Convention in furthering the notion State's are not responsible *per se* to the protection of the rights of privacy outside of their jurisdiction and territory which reveals weakness to such an interpretation compared to the ICCPR under the framework described above. What is important to understand from the *Soering* interpretation on extraterritorial application is that "jurisdiction" sets a territorial limit on the "reach of the Convention" in that not only does the Convention "not govern the actions of States not Parties to it" but it also does not "purport to be a means of requiring the Contracting states to impose Convention standards on other States."[180] Therefore, because Member States in this way are not obliged via this interpretation of extraterritorial application of rights within the Convention, the Council of Europe members essentially could conduct extraterritorial surveillance on an interpretative basis of the law to nations that are not within the Council of Europe due to such language in *Soering.* In *Bankovic and Others v. Belgium and Others* it is

[179] *Supra*. ECHR Art. 3.
[180] ECtHR. *Soering v. United Kingdom.* no. 14038/88. Par. 86. 7 July, 1989.

stated that only "exceptional circumstances" warrant the permissibility of performing acts outside of their territory constituting an exercise of jurisdiction.[181] Therefore, the language of the case-law still does not address the concern of extraterritorial surveillance could be conducted outside of the Contracting states and that such a concern under Article 1 of the Convention inherently limits the interpretation of the right to private life and correspondence under Article 8 should such an interpretation hold. Additionally, there is this language that states are to recognize the Convention standards that are within their own territory and under Article 8 this could be interpreted that the right to "private life" is a right that could be limited in scope on a per State basis if each State does not function by the same standards. Furthermore, States not operating under the same standards of the Convention leaves interpretation of human rights as variable per each State which could potentially reveal some of the inherent issues under the interpretation of jurisdiction under Article 1 of the ECHR and thus the effects it could have on the right to private life.

Comparably, the ICCPR under Article 2(1), which is pointed out clearly in General Comment No. 31, states that anyone within the "power or effective control of that State Party, even if not situated within the territory of the State Party" must have their rights, as stated in the Covenant, respected and ensured.[182] This interpretation from the Human Rights Committee almost appears to be very much opposite to the understanding of jurisdiction under the ECHR perspective. While Article 2(1) of the ICCPR is similar to Article 1 of the ECHR in this context in that they both provide territorial scope, the difference exists in the key aspect highlighted above of being "even if not situated within the territory…" as this also recognizes that the rights of *all* individuals are to be protected under the ICCPR while under the ECHR the rights within the Convention are limited to the Council of Europe Member States and are essentially confined to a "regional sphere."[183] Therefore, it is fair to conclude that the territorial applicability of the Human Rights Committee under the ICCPR applies to all humans, regardless of nationality, jurisdiction, or territory, and therefore recognizes the need to protect and ensure the rights of all and presents increased competency of privacy protections at the international over Council of

[181] ECtHR. *Bankovic and Others v. Belgium and Others*. no. 52207/99. Par. 67. 20 October, 1999.
[182] Supra. CCPR/C/21/Rev.1/Add.13, Par. 10.
[183] ECtHR. *Al-Skeini and Others v. The United Kingdom*. no. 55721/07. Par. 74. 7 July, 2011.

Europe level. However, the scope of such protections could be inherent to the issue of United States discussions on the matter which, as just shown, could perhaps be partially due to the wide scope of how jurisdiction applies in the ICCPR.

In *Banković and Others v. Belgium and Others* it was also noted that the "jurisdictional competence of a State is primarily territorial"[184] while furthermore establishing under doctrine of jurisdiction in international law that although State's are not forbidden under international law from "exercise of jurisdiction" extraterritorially, they are "limited by the sovereign territorial rights of the other relevant States."[185] This altogether establishes that "a State may not actually exercise jurisdiction on the territory, and thus normal public powers of the State, of another unless as a "consequence of military occupation"[186] or without the latter's consent, invitation, or acquiescence."[187] We are more concerned about the second aspect in the last statement rather than the first pertaining to consequences of military endeavors. Generally, the cases relevant to our analysis are more consistent to the argumentation of "consent" or even "acquiescence"; however, having said that, as a consequence of military action in *Issa and Others v. Turkey* the applicants argued the United Kingdom was an Occupying Power bound by the Geneva Convention and Article 43 of The Hague Regulations in restoring and ensuring public order while respecting laws in force of the country.[188] It was also noted here that the customs of the resident population could clash with securing the Convention rights outside of the area of the Council of Europe and the role was to respect laws in place and not to introduce laws and means to enforce them as stated by the applicants.[189] However, taking the interpretation of the ECHR under Article 1 that we have provided above, in this case, the notion of "effective control" in application of extraterritorial interpretation to the Convention to constitute jurisdiction did not hold.[190] Therefore, this potentially illustrates an idea that States may operate under what would be defined as "jurisdiction" of the Human Rights Committee context, but under the ECHR, such

[184] *Supra*. *Bankovic*. Par. 59.
[185] Ibid.
[186] *Supra*. *Banković*. Par. 71
[187] *Supra. Banković*. Par. 60
[188] ECtHR. *Issa and Others v. Turkey.* No. 31821/96. Par. 129. 16 November, 2014.
[189] Ibid. Par. 129.
[190] *Supra. Al-Skeini.* Par. 87

an interpretation leaves much to be determined as to what extent does "effective control" have to be in action in order to fulfill the notion of jurisdiction under the ECHR.

But like our comparison with the ECHR and the ICCPR above on jurisdiction, here it is applied no different. By ruling that there was no jurisdiction under Article 1 of the ECHR, this leaves us to question whether this would be applied to the Article set out in the ICCPR. Noted above, in *Al-Skeini,* it was determined that the United Kingdom was not in "effective control" either, which under general comment No. 31 on Article 2(1) would be the necessary to fulfill this criteria of jurisdiction under the perspective of the Human Rights Committee. Moreover, in this instance, neither the ECHR or the ICCPR applied to defend the position of the applicants. This allows us to perceive that perhaps under similar circumstances on extraterritorial surveillance that States not parties to the Council of Europe, could be subject to unpraiseworthy surveillance practices, while the ICCPR recognizes that the rights of the individual does not merit a nationality and thus would be potentially be defended under the discretion of this international framework. In an attempt to rectify this perhaps perspective that human rights merits a territorial or jurisdiction aspect in the *Al Skeini* case, the concurring opinion of Judge Bonello stated "jurisdiction" means nothing more than "authority over" and that one can have authority and control but would be imposture to claim to not recognize a breach in human rights because the party did not have jurisdiction.[191]

Extraterritorial application of surveillance is interpreted under the ICCPR's article 2, section 1, for states to respect the rights of individuals within its territory and also within its "jurisdiction".[192] In order to fully understand the scope and interest of extraterritorial application of surveillance, it is important to bring in to discussion the role of the United States to this matter, as obliged under the Vienna Convention on the Law of Treaties (VCLT)[193], and thus their involvement and interpretation of Article 2, Section 1, of the ICCPR, and therefore how they fundamentally approach the right to privacy not just for the sake of their own citizens, but

[191] *Supra. Al-Skeini.* Concurring Opinion of Judge Bonello, Par. 12.
[192] *Supra.* ICCPR. Article 2, Section 1.
[193] *Supra.* VCLT, Article 1.

potentially for anyone outside of the United States territory if even the ICCPR can be interpreted in an extraterritorial meaning.

The matter at which the ICCPR can be interpreted to apply extraterritorially at all seems to be the core of the matter it thinking of jurisdictional problems. In looking at the *Travaux preparatoires* of the ICCPR it appears as though there may be no clear sentiment on the matter that the ICCPR should or should not include extraterritorial application because of the little understanding and application of the matter at the time.[194] However, as time progressed, there is the possibility that as the war on terror grew, so did too the need for the States to consider all matters of potential intelligence gathering or surveillance remaining firm to the position to the Human Rights Committee that the ICCPR cannot be applied extraterritorially.[195] The United States, for example, has been clear in its statements to the Human Rights Committee of its interpretation of the covenant not including an extraterritorial application and that they do not share the view of extraterritorial reach that the Human Rights Committee has.[196] The Committee, in perhaps a landmark application of territory, found that it would be "unconscionable" to interpret article 2 "as to permit a State party to perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory."[197] This application of the rights on territories, other than the state party, of another member of the Covenant, draws an interconnected web of the protection of the right therein the covenant shared between all members; however, if the matter were that simple, then the United States, as shown above, would not reject the interpretation of article 2. Does this perhaps mean that the United States violates article 1 of the Vienna Convention on the law of Treaties? It may appear so, as not recognizing the rights that they claim to uphold on their own of privac

[194] Milanovic, Marko. Blog of the *European Journal of International Law*. "Comparing the ICCPR and the ECHR". Par. 6. 26 November, 2013.
[195] Ibid. Par 13.
[196] HRC. Third Periodic Reports of States Parties, 2003, U.S.A. Sec. 486.
[197] *Supra.* HRC. Delia Saldias de Lopez v. Uruguay. 1984.

Some of the issues that accompanies the right to privacy in extraterritorial surveillance When we are thinking of the individual being able to upload their personal information online, profile it online, they also potentially are making themselves vulnerable to nations that do not uphold protections to privacy- keeping in mind that information flows through national borders quite fluidly[198]

D.) Mass-Data Collection under International Law

In the concluding observations from the Human Rights Committee on the fourth periodic report of the United States, the Committee requests the U.S. to review its legal standing on extraterritorial application of the Covenant under certain circumstances further highlighting General Comment No. 31.[199] Furthermore, the Report essentially recognizes the that there is indeed a international legal character to extraterritorial application of the ICCPR, and that "under certain circumstances" which we can fairly prescribe to surveillance practices, the role of Article 2(1) on jurisdiction and territory, in addition to Article 17 on privacy, demonstrates that we can indeed apply and conclude that the ICCPR possesses an inherent legal character as it pertains to privacy rights in extraterritorial surveillance. In keeping with the compliance of the hypothesis, Mass-Data Collection under international law in the ICCPR is believed to be more protective to the right to privacy in the digital age than under the ECHR. To explore whether or not this stands true, the methodology of approaching the matter via the ECtHR will continue to take follow which will then draw to a conclusion as to the how the scheme of mass-data collection operates under the purpose of our analysis based off such findings.

The ECtHR possesses in its case law measures to protect the right of privacy; however, there stands the question if to what extent if possible, such protections to privacy exist, and if they do exist can such protection to mass-data collection be protected under international law? Mass-data collection essentially encompasses a wide array of the case-law that has been present throughout every chapter and sub-chapter as it plays an inherent role on the right to privacy in

[198] Berman, Jerry. "Privacy in the Digital Age: Work in Progress". *Nova Law Review.* Vol. 23. Pp. 554. 1998. Web.
[199] HRC. U.S. 4th Periodic Report, 2004.

the digital-age. Although collection of data, as was seen in the previous chapters, does occur at the individual level, in principal the collection of information does not necessarily have to occur, or be limited, to the individual level.

Different aspects of these cases were explored, whether that be on the functionality of privacy within the case-law, surveillance practices, surveillance procedures, or even territory; however, this exploration of case law on the digital age would be incomplete without establishing a stricter vision on the concept of collecting data in mass form and what repercussions under international and European human rights law this phenomenon perhaps has, if any at all. The relationship mass-data collection has with privacy and the digital age has been a theme throughout this piece, however, just to reiterate, we are referring to personal information as what is relevant in interpreting "data" in this sense, and what it means when parties, or States, take large quantities of personal information in bulk quantities and store or use it for a multitude of reasons that will be explored. Although much of this perspective already falls under the legitimate action and arbitrary action sub-chapters previously stated, this section will simply outline the principal of collecting data in mass-form rather than delving further into other aspects of the case-law that pertains to the process of surveillance as was already stated. Therefore, the point in addressing "mass" data collection via the CJEU and the ECtHR is to draw distinctions to its applicability to international law, if it can apply at all, to the protection of privacy under Article 8 of the ICCPR.

In *Klass and Others v. Germany*, there were five German lawyers regarding legislation in Germany empowering authorities to monitor their correspondence and telephone communications without obliging the authorities to inform them of the measures taken against them. In this case, the court held that due to the circumstances under which the G10 was operating, it did not contravene Article 8 in authorizing secret surveillance.[200] Such circumstances were found, as expressed in the earlier chapter, as fulfilling the criteria of what is "necessary within a democratic society." Therefore, as one could assume, the repercussions of such logic of secret surveillance measures could be quite astonishing depending on the justification for reasons, such as national security or public safety, as reasons that had been held

[200] *Supra Klass*. Par. 75

before for conducting these secret operations. What is not clear is the scope and intensity of the measures that these States would conduct the matter; whether the fact that it was not just targeted to an individual but an array of individuals all at the same time. It could be possible that States have reason for monitoring secretly thousands of people for the same reason that of course, as stated above, was not only "in accordance with the law" but also "necessary in a democratic society", and that individual, or those thousands of people, under the law, does not need to be required to be notified before, during, or after the operation for elements of maintaining secrecy. We therefore amount trust to State's to uphold the right to privacy when it comes to collecting personal information and monitoring, even in mass-form, as one would never know if they were a victim of those measures- regardless if the argumentation of the relevant authority would be that only those that would be monitored are those that actually could potentially be an existential threat to democracy. In conclusion, although it could be very well argued that it is in the State's best interest, for perhaps public approval or trust, to not conduct such arbitrary investigations, there does not appear to be

Furthermore, despite the large time gap between cases, *Weber and Saravia v. Germany* also presents an interesting parallelism in the defense of the states actions for collecting information. Here, with the amended G10 Act, the court felt there were adequate and effective guarantees against the abuse of the state's "Strategic monitoring powers" and found that interference was conducted in a way "necessary in a democratic society"- therefore fulfilling both of the conditions under Article 8(2) as explored above. Therefore, at least under the supervision and monitoring measures, the interpretation of what was indeed necessary in a democratic society under the *Klass* case decades before it, was ruled to be exactly the same given the detailed monitoring measures in the Parliamentary Supervisory Board, the authorization from the Feneral Minister, to the G10 Commission's overall role in the process.[201] However, although this may have been ruled similarly, it is important to note the clear difference on the subject matter. Since the *Klass* case, there have been clear advancements in communicative technologies that have widened the prospect of potential interferences and thus attracts "the Convention protection of private life more acutely."[202]

[201] *Supra.Weber and Saravia*. Par. 117.
[202] *Supra. Sazbo and Vissy.* Par. 53.

However, what does, and could demonstrate as arguable the most troublesome instances to the violation of Article 8 of the ECHR, or potentially Article 17 of the ICCPR, is when there exist domestic legislation that could leave the relevant intelligence, or surveillance authorities in question, unchecked with virtually infinite powers that protected surveillance measures from not only leaving citizen's without the "foreseeability" requirement as explored in the earlier chapter, but also collecting information to an extent that simply costs the human rights of thousands under a single instance. Altogether, in situations where "the legal discretion granted to the executive for the physical capture of external communications" as being "virtually unfettered"[203] exemplifies the potential tragedy to privacy rights in mass scale that such European and international laws, and of course norms, that have been put in place, fears would occur to the rights of individuals.

When we simply compare the interpretation of the ECHR and the ICCPR under this context of data collection in mass-form, we perhaps have some conflicting argumentation based on what has been presented above. This conflict is in this idea that the rights of individuals, and the interpretation of jurisdiction, creates a legal phenomenon that in international human rights law is not very well understood. The conflict is presented in a way where collection of mass data could potentially, and most likely, is collected from the same actor within the Council of Europe in addition to members of the ICCPR at the same time and approaches the protection of rights of the individual depending on the jurisdiction that the initiating actor is located in. The ECHR has been interpreted, as shown above, that if the information collected as "in accordance with the law" and reasonable "in a democratic society" then it was permitted for those actions; however, the law does not state how this principal should apply to outside the Council of Europe except for the fact that the Convention only protects State parties within the Convention. Since the ECHR does not have provide State's with the jurisdiction to adjudicate the rights of individuals outside its jurisdiction, therefore the Council of Europe, it is fair to say in the actions in the hypothetical context would not legally fit in the usage of Article 1 of the ECHR.

[203] *Supra. Liberty and Others v. The United Kingdom*. Par. 64.

Simply put, the collection of data in mass form, in order to protect the right to privacy in this era of cyberspace, mass surveillance, and extraterritorial surveillance, one must only approach the protection of personal information and jurisdiction of the right beyond the territorial confines of a region and must be taken at the international level to hold the truest merit of defense to the right to privacy. Furthermore, the ICCPR fulfills in this context our hypothesis to its applicability to mass-data collection based off of the information presented on its legal framework in addition to being able to consider the functions and operation of the case law presented. However, it is not believe that the case-law from interpreted from the ECHR would be viewed in the same way under the interpretation of jurisdiction under Article 1 of the ECHR for the same reasoning as the territorial issue. The ECHR therefore is argued to be insufficient in grounds for protection of mass-data collection compared to the international legal framework, in that of especially how it it applies in the digital age.

In conclusion on extraterritorial surveillance, the lack of case-law on specifically address mass-data collection, extraterritorial surveillance, and especially privacy rights related on the matter, the omission of its discussion in the law warrants a greater need for international binding materials given the apparent presence of the serious consequences of this type of surveillance, its unequivocal presence in the digital age, and the future ramifications that it can have on human rights altogether should the future of data protection no timely address this concern.

Conclusion,

In essence of our hypothesis and question, as to whether the right to privacy in the digital age could indeed exists is indeed a circumstantial question, and as explored both by through the interpretation of the ECHR, under the founding principle, laws, and Conventions, in addition to the like respective documents in relevance to the ICCPR, this is no easy question to be answers. Our hypothesis was to assess that the Council of Europe, because of the discourse on the matter, does not possess the adequate safeguards to the right to privacy in the digital age and because of the this, I believed that the ICCPR functions to respect this right in a greater, more applicable, and more detailed manner in relevancy to the global scope of the Covenant's application. I therefore applied case law from the ECtHR, under the right to privacy under Article 8 for certain procedures within surveillance, to see how this would function under Article 17 of the ICCPR. In conclusion, I believe that when it comes to the procedural safeguards, the ECHR is indeed perhaps lacking language to that of the protections under the ICCPR. Nevertheless, as was explored in extraterritorial application of the law, both the ECHR and the ICCPR both possess severe short comings, as especially to the collection of data in mass form, that has still much to be explored and thus I cannot hold my hypothesis holds merits within that context of application of the second major analysis chapter on territory.

Perhaps there is adequate legislation as we have may have seen above, but then that would mean that there is perhaps more of an implementation problem if the most adequate protective measures are in place which furthers a potential issue with accountability measures. Perhaps there is sufficient international and regional law to address the necessary legal language on the right to privacy but there isn't enough law domestically for enforcement and the necessary protections to safeguard privacy in the digital age at a tangible form.

There accompanies this idea that privacy exists in principal from the construction of community norm creation and that rights are protected by protecting the norms of social sphere where personal identity might be at stake.[204] This is potentially worth noting that earlier we address personal identity could be attached to personal information, and social sphere that perhaps exist in cyberspace as a "social culture", including Facebook, Twitter, and the like, that

[204] Devries, in reference to Robert Post.

then the protection of privacy need not only be recognized, but protected as an entity in greater form.

In somewhat of a sobering fact behind the right to privacy in the digital age is that protection of personal data is beyond the scope of absolute governmental control or protection. Personal information could be vulnerable to a multitude of individuals and actors across the world, but what we were exploring throughout this paper is what are the current safeguards that are in place to protect privacy in the digital age and what can we understand from the character of surveillance to unveil what

As can be seen, the application of our rights and freedoms has evolved dramatically as argued because of the advancements in communication technologies. The degrees of separation between humans is much lower than what it ever used to be and upholding the right to privacy and the freedom of expression should not take for granted this evolution. In the analysis explored above, key case law, legal scholarly articles, and relevant information on the right to privacy as it pertains to surveillance we deepened the conversation and updated the status of his right as applied via international and regional laws and conventions. We hypothesized there was a legislative deficit to safeguard the right to privacy in the digital age; however, after going through the case-law and studies, we discovered that the approach to privacy in surveillance is still being understood legally and is handled on a per case basis. We found that this means because of the approaches to safeguards, extraterritorial application and dangers, arbitrariness, and issues with legitimacy, the application of virtual rights to international law, and the simple lack of legal and defining character to key terms within surveillance's application to privacy, that there indeed does exist such a deficit and it does, and continues, to pose a risk for the longevity of human rights.

Bibliography,

Australian Bureau of Statistics. "Statistical Language: What is Metadata". 3 July, 2013. Web. < http://www.abs.gov.au/websitedbs/a3121120.nsf/home/statistical+language+-+what+is+metadata>

Berman, Jerry. "Privacy in the Digital Age: Work in Progress". *Nova Law Review.* Vol. 23. Pp. 554. 1998. Web.

Brandeis, Louis D. "The Right to Privacy" *Harvard Law Review*, Vol. 4, Issue 5 , Pp. 193-220. 1890.

Bundesnachrichtendienst. G10 Commission. http://www.bnd.bund.de/EN/Scope_of_Work/Supervision_and_Control/G10_Commission/G10_Commission_node.html

Bundesamt für Verfassungsschutz. "Parliamentary Control" Par. 9.

Chander, Anupam. "United Nations General Assembly Resolution on the Right to Privacy in the Digital Age". *International Legal Materials,* Vol. 53, Issue 4 (2014), Pp. 727

CJEU. *Google Spain and Google v. AEPD.* Case, C-131/12. Par. 19, 22. 13 May, 2014.

Cole, David and Federico Fabbrini. "Bridging the Transatlantic Divide? The United States, The European Union, and the Protection of Privacy Across Borders." *Oxford University Press.* ICON, Vol. 14. No. 1. Pp. 221.

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, Article 8, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

Council of Europe*, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, Art. 2. 28 January 1981, ETS 108.

Deeks, Ashley. "An International Legal Framework for Surveillance." *Virginia Journal of International Law.* Vol. 55. Pp. 400. 2015. Web.

DeVries, Will Thomas. "Protecting Privacy in the Digital Age." *Berkeley Technology Law Journal*, Vol. 18, Issue 1. Pp. 285, 286. 2003.

ECtHR. *Ahmet Yildirim v. Turkey*, no. 3111/10, 18 December, 2012. Recommendation III.

ECtHR. *Al-Skeini and Others v. The United Kingdom*. no. 55721/07. Par. 74. 7 July, 2011.

ECtHR. *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria.* No. 62540/00. Sec. 6. 28 June, 2007.

ECtHR. *Barbulescu v. Romania.* no. 61496/08, Dissenting Opinion, Justice Albuquerque. Par. 5. 8 April, 2014.

ECtHR. *Bankovic and Others v. Belgium and Others*. no. 52207/99. Par. 67. 20 October, 1999.

ECtHR. *Issa and Others v. Turkey.* No. 31821/96. Par. 129. 16 November, 2014.

ECtHR. *Kalda v. Estonia.* no. 17429/10. 19 January, 2016.

ECtHR. *Kennedy v. United Kingdom,* no. 26839/05, 18 May, 2010 Par. 118.

ECtHR. *Klass and Others v. Germany. no. 5029/71.* Par. 42. 6 September, 1978.

ECtHR. *K.U. v. Finland*. no. 2872/02, B. "The Court's Assessment", 2 December, 2008 Par. 42.

ECtHR. *Kvasnica v. Slovakia* no. 72094/01 Par. 80. 9 June, 2009.

ECtHR. *Liberty and Others v. The United Kingdom*. no. 58243/00 Par. 59. 1 July, 2008.

ECtHR. *Roman Zakharov v. Russia.* no. 47143/06. Section 154. 4 December, 2015.

ECtHR. *Soering v. United Kingdom.* no. 14038/88. Par. 86. 7 July, 1989.

ECtHR. *Szabo and Vissy v. Hungary.* no. 37138/14. Par. 68. 12 January, 2016.

ECtHR. *Weber and Saravia v. Germany. no. 54934/00.* Par. 101. 10 January, 2000.

Encyclopedia Britannica. Extraterritoriality. International Law. Access 22 July, 2017.

European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995.

European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02.

European Union. *"*On the lawful Interception of Telecommunications" Council Resolution 96/C 329/01. 17 January, 1995.

European Union. Directive 2002/58/EC, Par. 5 31 July, 2002.

European Union. Regulation 2016/679 Par. 9. 27 April, 2016.

Government of Canada. "Canada's Cybersecurity Strategy. Pp.2 2010.

Human Rights Council. 28th Session. Sec.1. "Summary of the Human Rights Council Panel Discussion on the Right to Privacy in the Digital Age". 19 December, 2014.

Human Rights Council. A/HRC/17/27. Special Rapporteur. 16 May, 2011.

Human Rights Council. A/HRC/RES/28/16. 1 April, 2015.

HRC. A/HRC/RES/28/16, General Comment No. 16. 4 January, 2015.

HRC. CCPR/C/21/Rev.1/Add.9 General Comment No. 27, 1 November, 1999.

HRC. CCPR/C/21/Rev.1/Add.13 General Comment No. 31. Par. 6.
Human Rights Committee. CCPR /C/USA/CO/4, Par. 22.

HRC. Third Periodic Reports of States Parties, 2003, U.S.A. Sec. 486.

HRC. U.S. 4th Periodic Report, 2004.

Human Rights Council. "The Right to Privacy in the Digital Age: Report of the OHCHR". 3 June, 2014.

International Court of Justice. "Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory." General List No. 131 Par.107-111. 9 July, 2004.

Kurt Young, Jr. "Privacy Law in the Digital Age: Establishing Privacy Rights in Search Engine Logs". *Connecticut Public Interest Law Journal*. Vol. 14, No. 1. Pp. 157.

Milanovic, Marko. "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" *Harvard International Law Jounral.* Vol. 56, No. 1. Pp.86. 2015.

Milanovic, Marko. Blog of the *European Journal of International Law*. "Comparing the ICCPR and the ECHR". Par. 6. 26 November, 2013.

OHCHR. "Your Human Rights: The Right to Privacy in the Digital Age". Par. 2. Access: 2 July, 2017.

OHCHR. "Special Rapporteur on the Right to Privacy". Access: 14 July, 2017. <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>

OHCHR. Human Rights Committee. Access: 4 July, 2017 <http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIndex.aspx>

Roagna, Ivana. "Protecting the right to respect for private and family life under the European Convention on Human Rights" *Council of Europe Human Rights Handbooks.* Pp. 44. Strasbourg, 2012. Web.

Russian Federation. OSAA Section 8(2). Russia. 12 August, 1995.

Savoiu, Alina. "The Right to Privacy". Annals of the "Constantin Brancusi" University of Targu Jiu, Juridical Sciences Series, Issue 1. Pp. 89. 2013.

United Nations, *Vienna Convention on the Law of Treaties*, Articles 31 and 32. 23 May 1969, United Nations, Treaty Series, vol. 1155, p. 331

UN General Assembly, *Convention on the Law of the Sea*, 10 December 1982.

UN General Assembly, *International Covenant on Civil and Political Rights,* 16 December 1966, United Nations, Treaty Series, Vol. 999, Articles 2, 17, 26, p. 171.

UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, 16 December 1966, United Nations, Treaty Series, vol. 993, p. 3

UN General Assembly. “The Right to Privacy in the Digital Age”. A/RES/Res/68/167. Par. 2, 11. 21 January, 2014.

UN General Assembly*, Universal Declaration of Human Rights*, 10 December 1948, 217 A (III)