CROSS BORDER PRIVACY RIGHTS: AN OVERVIEW IN REFERENCE TO THE HILLARY CLINTON CONTROVERSY

ABSTRACT

The Right to Privacy has been recognized as a basic human right across the globe. Article 17 of the International Covenant on Civil and Political Rights guarantees the Right to Privacy and states that 'individuals have the right to share information and ideas with one another without any interference by the State, secure in the knowledge that their communication will reach and be read by the intended recipients alone'. The right may not be given explicitly in certain States, such as India where the Courts derive the right from a set of subsisting rights. The enforcement of the Right to Privacy is a complex issue. More so, when the issue raised is about a State official's usage of his private communication network for official duties. The question is to what extent a State can breach the right to privacy under the guise of security concerns and whether it can extend to monitoring or examining even personal aspects of the communication wholly unrelated to the State. This Article shall contain an amalgamation of the current International laws and trends pertaining to the issue and shall give solutions to the same.

Keywords: International Covenant on Civil and Political Rights, Privacy, Right, State.

INTRODUCTION

Communication, since time immemorial, has been an important aspect of human life. It is used to convey ordinary, everyday messages as confidential information. The key feature of communication is that it is universal in nature and although it has several forms and mediums of expression, it remains vital.

The evolution of documented communication has risen from paper to oral recording devices to modern day communication of phone calls, text-messages and e-mails. These communication methods are not limited to certain persons or functions. Modern day communication is truly universal in nature, in all regards. It is used by every individual whether for personal, professional or State use. The protection of such communication was earlier limited to physical protection of such documents from the possession of unwanted elements. In the modern scenario, however, protecting an individual's right becomes a

difficult proposition due to an increase in the illegal and unauthorized methods of gaining access to a person's private communication such as hacking.

The issue in this Article revolves around the usage of private communication networks by State Officials who correspond with multiple people. However, State Officials also have private lives and tend to mix the two spheres for want of convenience to be able to attend to both spheres of their lives on a single device. Hillary Clinton's Presidential campaign was shrouded in controversy due to alleged Russian hackers releasing her private and State correspondence emails involving arming Jihadists in Syria to WikiLeaks[1]. This led to an investigation by Federal Bureau of Investigation where she had to turn in 30,000 emails sent through her private email server which she used according to the rules and regulations.[2]Although the facts of the matter are circumstantial, the paper is operating under the pre-texts that the alleged Russian hackers could either be State controlled or were non-State actors. Thepaper shall attempt to answer the following questions:

1. Do cross border privacy rights exist?
2. Where would jurisdiction lie?
3. Is cross border espionage legal?

The Hypothesis of the research is that a National Security concern shall override the Right to Privacy of an individual irrespective of whether the said person adheres to the rules set for using private communication networks for Official State actions.

SCOPE OF PRIVACY RIGHTS IN THE INTERNATIONAL SPHERE

The treaties of the International Covenant on Civil and Political Rights (ICCPR)[3] and the European Convention on Human Rights (ECHR)[4] protect the Right to Privacy. They closely followed Article 12 of the Universal Declaration of Human Rights. Article 17 of the ICCPR provides that:

---

[1] *18 revelations from Wikileaks' hacked Clinton emails*, BBC News (May 9, 2017, 10:05 AM), http://www.bbc.com/news/world-us-canada-37639370.
[2] Robert O'Harrow Jr., *How Clinton's email scandal took root*, Washington Post (Apr. 28, 2017, 05:45 PM), https://www.washingtonpost.com/investigations/how-clintons-email-scandal-took-root/2016/03/27/ee301168-e162-11e5-846c-10191d1fc4ec_story.html?utm_term=.fafb0b9aded3.
[3] *International Covenant on Civil and Political Rights*, United Nations Human Rights Office of the High Commissioner (Apr. 12, 2017, 08:09 PM), http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.
[4] *The European Convention on Human Rights*, European Court of Human Rights, (May 28, 2017, 11:27 AM) http://www.echr.coe.int/pages/home.aspx?p=basictexts.

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

On the other hand, Article 8 of the ECHR states that:

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 prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others.*

These provisions are largely vague in nature. In an attempt to reduce ambiguity, Brazil and Germany submitted a draft Resolution titled "The Right to Privacy in the Digital Age" to the Third Committee of the United Nations General Assembly.[5] The Assembly's Resolution on the right to privacy in the digital age, symbolized a major development as it brought the issue of electronic surveillance within the ambit of international human rights law. It gives direct reference to and invokes both Article 12 of the Universal Declaration of Human Rights and Article 17 of the ICCPR. It noted that the rapid pace of technological development enhances the capacity of Governments and individuals to intercept data 'which may violate human rights, in particular the right to privacy'.[6] Operative paragraph three and four state that 'the same rights people have offline must also be protected online'[7] and 'respect and protect the right to privacy, inclusive of the context of digital communication'[8] respectively.

[5] *Brazil, Germany submits draft resolution on Right to Privacy*, Global Policy Forum (May 28, 2017, 12:13 PM), https://www.globalpolicy.org/global-taxes/52534-brazil-and-germany-submit-draft-resolution-to-general-assembly.html.
[6] *The Right to Privacy in the Digital Age*, United Nations General Assembly (Mar. 28, 2017, 07:07 PM), http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45.
[7] *Resolution Adopted by General Assembly on 18 December 2013 68/167. The Right to Privacy in Digital* Age, United Nations General Assembly (Mar. 28, 2017, 07:46 PM), https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf.
[8] *Id.*

An examination of the travaux during the drafting stages shows that there was a 'complete lack of conceptual coherence'.[9] Although the issue of territorial scope was discussed, many States were concerned about the manner in which the Covenant would apply to some complex scenarios such as protection of the Nationals living abroad, etc.[10] The travaux made no indication that there would be a lack of extraterritorial applicability. The same was reiterated by the International Court of Justice (ICJ) in the Wall case[11] where the Court stated in the ratio of 14:1 that the ICJ would have an advisory jurisdiction under Article 17 of the ICCPR.

However, the same case saw a strong categorical opposition from the United States of America (U.S.A.). "It is the long-standing view of U.S.A. that the Covenant by its very terms does not apply outside of the territory of a State Party."[12] The opposition of U.S.A. to extraterritorial application has been met with heavy criticism. U.S.A. states that the ICCPR is vague and is open to several possible interpretations using the rules of interpretation described in the Vienna Convention on the Law of Treaties.[13]

Therefore, the scope on the applicability of Article 17 of the ICCPR poses complex problems due to the ambiguousness owing to the countries such as U.S.A. taking a stand against the applicability of the Conventions extraterritorially. This would pose a problem if the U.S.A. chose to take action against Russia as it would involve changing their position on applicability of the Conventions.

JURISDICTIONAL MODELS UNDER INTERNATIONAL LAW

The concept of State jurisdiction on human rights treaties is complex with different States adopting different models. The Spatial model of jurisdiction talks about a State's control over an area whereas the personal model deals with control over individuals. The case laws on extraterritorial application offer different opinions as well as there seems to be no particular consensus on the topic.

---

[9] Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age* (Mar. 29, 2017, 10:07 AM), https://www.ilsa.org/jessup/jessup16/Batch%202/MilanovicPrivacy.pdf.
[10] *Id.*
[11] United States v. Israel, 2004 I.C.J. 136 (Hague).
[12] Kevin Jon Heller, *Does the ICCPR Apply Extraterritorially?*, Opinio Juris (Mar. 29, 2017, 12:03 PM), http://opiniojuris.org/2006/07/18/does-the-iccpr-apply-extraterritorially/.
[13] Milanovic, *supra* note 9, at 107.

Spatial Model

The model's applicability is linear in nature and deals with de facto control over areas under the control of the State.Firstly, if an individual is present in an area that the State can exercise control over and the individual's right to privacy is affected in one of these areas, it will be the State's responsibility of ensuring the right.[14]

Thus, if Narendra Modi was in Washington City visiting the President, and an agent from National Security Agency searched his room, interfering with his phone, laptop or any other means of communication remotely, the United States of America would be liable if India communicated an objection to the ECHR. However, it may not necessarily be unlawful but U.S.A. would need to justify their actions. Under the model, the State must have control over the territory and therefore, if the same happened while any dignitary from another State were to visit Iraq during its occupancy by U.S.A.

Secondly, the State must exercise due diligence and take any and all reasonable measures including technological measures necessary to ensure such situations can be mitigated to a reasonable extent. For example, mandating the use of encryption when transmitting personal data.[15]

The model was discussed in the Bankovic case where the Court stated the terms that, "It is difficult to contend that a failure to accept the extra-territorial jurisdiction of the respondent States would fall foul of the Convention's order public objective, which itself underlines the essentially regional vocation of the Convention system. In short, the Convention is a multi-lateral treaty operating in an essentially regional context and notably in the legal space (espacejuridique) of the Contracting States."[16]

The benefit of the Spatial model lies in its clarity. The jurisdiction under the model is straightforward. However, the model offers no insight on modern day problems. For example, if Narendra Modi sends an email from India to U.S.A. and it is intercepted in

[14] Marko Milanovic, *Foreign Surveillance and Human Rights, Part 3: Models of Extraterritorial Application*, EJIL: Talk! (Mar. 30, 2017, 02:53PM), https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-3-models-of-extraterritorial-application/.
[15] Milanovic, *supra* note 9, at 123.
[16] Cedric Ryngaert, *Clarifying the Extra-Territorial Application of the European Convention of Human Rights (Al-Skeini v. the United Kingdom)*, Utrecht Journal of International and European Law (Mar. 30, 2017, 04:29 PM), https://utrechtjournal.org/articles/10.5334/ujiel.ba/galley/27/download/.

Germany where the e-mail server is located, which country has jurisdiction to try the case, India, the U.S or Germany? The model serves no clarification on the question.

Personal Model

The Personal Model is in reference to when the State through its agents exercises control and authority over an individual.[17] The limitations of territory do not apply here. For example, a German diplomat in a foreign country like Australia interfering and exercising control over Malcolm Turnbull's communication would come under German jurisdiction and therefore, would be liable with respect to any breaches of privacy under Article 17 of the ICCPR or Article 8 of the ECHR.

After Bankovic case, the question of extraterritorial applicability was brought forward once again in *Al-Skeini & Ors.* v. *United Kingdom*[18] and was widely expected to abandon the strict Spatial Model adopted. Although the case confirmed the validity of the State-Agent authority model (Personal Model), it did not categorically state that an individual over whom an ECHR Contracting State exercises control or authority falls, as a matter of course, within that State's jurisdiction for purposes of the application of the ECHR.[19]

Prima facie, the personal model appears reasonable with a strong moral appeal and should've been embraced. However, it is not free from criticism. An unrestrained personal model may cast the net too wide and unjustifiably increase the obligations.[20]

U.S.A., therefore, clearly adheres to the Personal Model where it shall claim responsibility of ensuring the Right to Privacy of its citizens only when it has been violated by an agent of the State and will not concern itself with when the violation was caused by a party not acting under their control.

ESPIONAGE UNDER INTERNATIONAL LAW

Espionage includes the use of State-controlled assets for the purpose of gaining information from a State with the aim to improve the knowledge of a competitor country.[21] International

[17] Supra, note 15.
[18] Al-Skeini & Ors. v. United Kingdom, [2011] ECHR 55721/07 (United Kingdom).
[19] Cedric, *supra* note 17, at 59.
[20] Cedric, *supra* note 17, at 60.

law only mandates a few codified rules but has no strict bar on the same[22] and any act of espionage is merely deemed 'unfriendly'.

Article 8 of the ECHR states that everyone has the right to respect for his private and family life, his home and correspondence, subject to certain restrictions that are in accordance with law and necessary in a democratic society. The term 'private life' is considered to be very broad which the Court has interpreted according to the facts of individual cases.[23]The crux of the various definitions set by the Court is a private space which noone can enter and has the right to be left alone from unwelcome interferences in a manner of one's own choosing.[24]

Therefore, acts of espionage attempting to interfere with any communication would be a violation of his right to private life including e-mail interception.

The Right to Privacy would come under the ambit of right to private life as well. Privacy can be defined as the ability to keep information secret. Article 8, quite rightly also incorporates the right to protection of personal data under the right to privacy[25] which protects correspondence 'expressisverbis'which is understood to include phone and email as well[26].

Protection of Residents against Espionage

Generally, States cannot be held accountable for acts by other States. But, a State is under a positive obligation according to Article 1 of the ECHR to 'take diplomatic, economical, judicial and other measures that are in its power to take and which are in accordance with International Law to secure rights guaranteed by the Convention'.[27] The text can be interpreted in two ways. Firstly, it creates a positive obligation to ensure the protection of human rights against violations by other States. Secondly, it compels the States to refrain from harming others.

---

[21]Stefan Kirchner, *Beyond Privacy Rights: Crossborder Cyber-Espionage and International Law*, 31 J. Marshall J. Info. Tech. & Privacy L. 369, 372(2014).
[22] John Kish & David Turns, International law and Espionage (1 ed. 1995).
[23]IlinaGeorgieva, *The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR*, Utrecht Journal of International and European Law (Mar. 31, 2017, 11:38 AM), https://utrechtjournal.org/articles/10.5334/ujiel.cr/.
[24] Petty v. United Kingdom, [2002] ECHR 423 (France).
[25]Christoph Grabenwarter, EuropäischeMenschenrechtskonvention 194 (3 ed. 2009).
[26] Kirchner, *supra* note 22, at 376.
[27]*Supra* note 4.

However, in certain situations, in the interest of National Security, State's claim to espionage is unavoidable as given in paragraph 2 of Article 8. To determine the legitimacy of such claims, the Court employs a 'fair-balance' test[28] where it weighs 'the interests of the community and interests of the individual'[29]. In principle, espionage is not illegal per se under international law as far as the relations between states are concerned.[30] The same is not applicable to a State attempting to gain access to personal data.

Therefore, according to Article 1 of the ECHR, U.S.A. has a positive obligation to question Russia's actions in the European Court of Human Rights for the violation of Hillary Clinton's right to privacy or deal with matter diplomatically or place economic sanctions on Russia. On the other hand, if Russia can justify their actions as 'necessary in a democratic society', they shall be immune to any action taken by U.S.A.

SUGGESTED SOLUTIONS

1. Jurisdictional Co-operation

To avoid Jurisdictional confusion, there are certain compliances that are followed by way of formation of contracts, giving consent and various other adequacy decisions. Instruments for privacy cooperation like the Council of Europe working parallel to the Organisation for Economic Co-operation and Development and Asia-Pacific Economic Cooperation which form certain cross border-privacy rules and guidelines that need to become binding on all the signatory nations avoiding arbitrary non-acceptance of jurisdiction in such matters.

2. Effective Recourse Mechanisms

The existing patchwork for enforcing jurisdiction in cross-border privacy cases has done little to protect individuals and government officials alike from breaches. A mechanism where the individual is compensated along with a sanction against the violator should be made mandatory.

3. Established Modus Operandi

The United States of America during the National Security Agency leaks due to international pressure was forced to issue an apology and make amendments to its National Security

[28] Dickson v. U.K., [2007] ECHR 1050 (France).
[29] See Kircher, *supra* note 22, at 377.
[30] *Id.*

policy. A majority of such cases are dealt with diplomatic arm twisting or an apology as the case may be. A pre-determined method must be implemented to deal with breaches of such nature where apart from diplomatic arm twisting, must also include adequate economic and legal sanctions to ensure future violations are not done arbitrarily.

CONCLUSION

The right to privacy of communication in the digital age is protected by Article 17 of the ICCPR and Article 8 of the ECHR owing to the draft Resolution introduced by Brazil and Germany in 2013 during the aftermath of the Snowden leaks. However, there seems to be a difference in the effectiveness of applicability between the two articles. Firstly, with respect to Article 17 of the ICCPR, there seems to be no consensus on the Jurisdictional models of Spatial and Personal. U.S.A. is also categorically opposed to the Spatial Model and will take no action or lay claim to any responsibility under it. In hindsight, Article 8 of the ECHR seems to have a wider ambit of applicability due to the definition of 'private life' encompassing a larger scope than Article 17 of the ICCPR

Espionage under international law is not illegal per se. Therefore, Russian acts can only be held as unfriendly. U.S.A. had come under heavy scrutiny by other States due to the revelations of the Snowden leaks. U.S.A. had to apologize for its actions and promised to lay down strict measures to ensure that no such unjustifiable actions take place in the future. Therefore, it is yet to be seen whether they would take up their obligation mentioned under Article 1 of the ECHR. An action, if any, would most likely be diplomatic and taken behind closed doors.

U.S.A.'s further intrusion into Hillary Clinton's emails to ascertain the extent of the security breach is also justified under Article 17 of the ICCPR and Article 8 of the ECHR which state that the actions are neither 'arbitrary and unlawful' or 'necessary in a democratic State in the interest of national security' respectively. Any recourse available to her is in the hands of State action against Russia.

Therefore, on the basis of arguments presented, research conducted and evidences presented in the paper, the authors are of the view that the hypothesis which the paper initiated has been affirmed in the end. The Authors believe that a National Security concern shall override the

right to privacy of an individual irrespective of whether the said person adheres to the rules set for using private communication networks for Official State actions.