****Approved Copy****

Human rights, international law and the right to privacy

Kristian P Humble, University of Greenwich, UK

Abstract

The right to privacy is the right to obscure or hide parts of an individual's life from the view of the wider public. An individual right to privacy is seen as a fundamental human right within the wider context of international law. In the age of surveillance from the state and private internet communications companies, for an individual to protect their privacy or to remain obscure is now becoming almost impossible. A renewed emphasis on the right to privacy influenced in direct response to the aftermath of the Edward Snowden and Cambridge Analytica revelations. The protection of privacy and the international community must address not only the practices of state sponsored surveillance but also surveillance undertaken by modern private communications companies. This article will focus on how the international community and international law is protecting the privacy of the individual in an increasingly fast moving area of rights protection and technological advancement.

Key words: Privacy, International Law, Rights, Surveillance, State, Human Rights, Digital Age, Communication.

Introduction

The right to privacy is a fundamental human right enshrined in the Universal Declaration of Human Rights (UDHR)[1] and the International Covenant on Civil and Political Rights (ICCPR).[2] The right to privacy is now being see as of greater importance in light of the Edward Snowden revelations in 2013 and Cambridge Analytica in 2018. The international community is now focused on addressing not only the practices of state sponsored surveillance but also surveillance undertaken by modern communications companies.[3] Even though there has been some improvement in this area, the protection of individuals privacy remains ambiguous.

The basis of the protection by the international community and the United Nations is the application and interpretation of Article 17 of the ICCPR and more recently in the United Nations Resolution on Privacy in the Digital Age.[4] The basis of the privacy protection debate is how to bring surveillance practices in line with human rights law and what privacy now means in the modern digital age. International law in essence holds states accountable for their actions (not in all cases) based on the effective control test.[5]

However now there needs to be an international legal solution not only to the behaviour of states, sometimes referred to as the Five Eyes[6] states but also by communication based private companies such as Facebook. Activities which use surveillance into individual's digital movement without an individual's permission is clearly in breach of Article 17 of the ICCPR.

What is privacy?

International law is trying to play catch up to try and regulate the growing concern for privacy protection as the international community has overall been slow in responding to changes in modern technologies, especially those that are based on communication and data collection.

Article 17 of the ICCPR 1966 sets out privacy as the following:

> 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.

In 1988 this was further expanded in General Comment No 16 on Article 17 ICCPR.[7] This Comment explained:

> 1. Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home or correspondence as well as against unlawful attacks on his honour and reputation. In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. The obligations imposed by this article require the State to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right.
>
> 2. In this connection, the Committee wishes to point out that in the reports of States parties to the Covenant the necessary attention is not being given to information concerning the manner in which respect for this right is guaranteed by legislative, administrative or judicial authorities, and in general by the competent organs established in the State. In particular, insufficient attention is paid to the fact that article 17 of the Covenant deals with protection against both unlawful and arbitrary interference. That means that it is precisely in State legislation above all that provision must be made for the protection of the right set forth in that article. At present the reports either say nothing about such legislation or provide insufficient information on the subject.

In 1966 the ICCPR was not adequately sufficient in scope to ascertain the threat to individual privacy from digital and data collection technologies because these technologies did not exist. The definition contained within the 1966 document is therefore is considered too narrow in today's technological advances in communication and data collection to be a full formed definition of the protection of privacy.

The 1988 General Comment only goes a little further to distinguish the incoming threat of data collection by states and the protection of states from individual's private data being interfered with. However, a full appreciation of technologies concerning communication and information were not fully appreciated as these technologies were only at their infancy.

The international community and the United Nations needs to look at updating the definition within the context of the modern digital age. This general discussion has been enhanced by the appointment of the United Nations Special Rapporteur Frank La Rue[8], whose sole aim is to report on the infringement of privacy at state level regarding individuals privacy protection.

The General Comment to Article 17[9] states that 'the gathering and holding of personal information on computers, databanks and other devices by public authorities or private bodies must be regulated by law.'[10] Article 17 guidelines have also been agreed upon by the Human Rights Committee (HRC)[11] and has been followed in a number of European Court of Human Rights (ECtHR) decisions.

Can we really keep ourselves private*?*

Privacy could be argued to be an essential human right as well as an essential human need. All individuals need the knowledge to understand that certain elements of their lives can be obscured or kept private, away from others. In the digital age with the constant reliance on digital communication, do we really have the right to keep ourselves obscured, or are we part of the process which gives up the notion of privacy?

Post has suggested the following:

> 'Privacy is a value so complex so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings that I sometimes despair whether it can be usefully addressed at all.'[12]

Rengel explained that:

> 'The concept of privacy involves a definition of what it entails as well and how it is valued, while the right to privacy refers to the recognition that privacy should be legally protected.'[13]

Privacy has consistently been defined in the context of personal autonomy or having the innate control over the personal intimacies or having control over the personal data which is available about oneself.[14] At its core privacy is about the protection of oneself from the outside world.

This need for obscurity or privacy can also be described as 'claim of individuals, groups or institutions to determine for themselves when how and to what extent information about them is communicated to others'[15] or 'privacy is the condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited.'[16]

Solove has put privacy into six different concepts:

(1) The right to be left alone.
(2) Limited access to the self, the ability to shield oneself from unwanted access by others.
(3) Secrecy, the concealment of certain matters from others
(4) Control over personal information, the ability to exercise control over information about oneself.
(5) Personhood, the protection of ones' personality, individuality and dignity and;
(6) Intimacy, control over or limited access to ones' intimate relationships or aspects of life.[17]

Solove's categories are a common sense approach to privacy that most individuals would agree that on some level all human beings need the right to be left alone. However, the problem exists in that some individuals will value some privacy actions over others. Some for example may not value intimacy as an important protection. This can be seen in the use of Instagram to catalogue personal images of oneself.

Solove's own unique definition of privacy is the following:

> 'The value of privacy must be determined on the basis of its importance to society, not in terms of individual rights. Moreover, privacy does not have universal value that is the same across all contexts. The value of privacy in a particular context depends upon the social importance activities that it facilitates.'[18]

Here, Solove is contextualising privacy, privacy which needs to change with time and maybe what privacy means to individuals and not the wider world's interpretation of it. This must and should be the basis of how the international community must view privacy. Newell went further and suggested that privacy can described in as a number of different protective rights, from control over personal information, freedom from surveillance, protection from invasions into someone's home, personal autonomy and control over one's body.[19]

The traditional right to privacy before the onset of the digital age presupposes that human interaction will often take place in the public sphere. This means that an individual will only give up their personal space when they feel safe to so and a right to be obscure is much easier to ascertain. In cyberspace obscurity is much more difficult to obtain. It has been stated that a right to obscurity in the digital age is not much more than a desirable goal and has little chance of being achieved in the reality.[20] Obscurity can be described as a 'state of unknowing or being unidentifiable online'.[21] Out in the public space it is impossible for an observer to identify someone's identity or personal data because they do not have the correct pieces of this personal puzzle to fit together as they do not have access to any personal information. For example, an observer who observes a conversation will be unlikely to ascertain any personal information about the individuals taking part in the conversation simply by observing them in a public space.

Online obscurity is much more complex; a person can remain obscure if a piece of vital personal information is missing like identity or social connections. However, with some of these vital personal pieces fitting together, like for example social connections, the online observer can, if they have right tools, infiltrate private information much easier than if they were observing a conversation taken place in a public space.

Obscurity therefore, would only be fully realised through regulation that protects an individual's information in which they wish to keep private. Therefore, if a right to privacy has been recognised within international treaties and national domestic legislation then surely obscurity is just another function of privacy.

Hartzog and Strutzman have suggested other frameworks that could lead to a protection of obscurity and protection of privacy on the internet.[22] They have suggested that the protection of obscurity may be easier to implement than that of a pure privacy recognition due in the main to the problematic nature of a widely accepted definition of a right to privacy. This would mean in essence instead of regulating websites to remove sensitive information, courts could propose some element of obscurity i.e. the individual must specifically mandate what information is to be made visible.

However, this still puts the individual information received and what to do with it in the hands of the receiving company, the trust of the company not to expose personal or sensitive personal information. In light of Cambridge Analytica this seems problematic. What is needed is a stronger legal mandate to obscurity on the internet.

Hartzog and Strutzman suggested four factors which could be used by the courts to determine whether some aspects should be deemed private or public. They suggested that if certain elements were missing from the public then they are closer to being obscure and should come with some element of a protection of privacy attached to them. These factors suggested are:

(1) Search visibility (ease of discovery in search systems)
(2) Unprotected access (degree of access restriction)
(3) Identification (degree to which individual is identified by direct or indirect disclosure)
(4) Clarity (ability for observer to comprehend or discover information)[23]

To expand the understanding of these four factors, Hartzog and Strutzman used the following scenarios:

> Scenario 1 is a blog that is visible only to invited users and is not searchable by general search engines like Google. It is close to being completely obscure because it is missing two of the most important factors for finding it. Scenario 2 is a Twitter account that uses only a first name and a blurry photo to identify the poster. While this information is more obvious than the information in Scenario 1 because it is freely searchable and accessible, it is still slightly obscure because only certain Internet users would be able to identify the poster of the content or completely comprehend any idiosyncratic posts.[24]

Therefore, these determining factors as suggested by Hartzog and Strutzman are based on which elements are present for the courts to deem them to be obscure. If a social media user identifies themselves by their name, posts a picture of themselves online in which they are easily identifiable then this cannot be a case of privacy and the individual cannot presuppose themselves as to be trying to be obscure. If (and it's a big if in light of our use of communication apps in social media) however, elements within these four factors are missing as in the scenarios used above, then the court could determine that there was an element of obscurity intended to be observed by the individual.

Both the right to obscurity and the right to privacy are interlinked but are not helped by the current international guidelines not being clear enough on the protection of these rights. But clear guidelines on obscurity in the definition of what is private and what is public could help in making the protection and what should be protected much clearer.

The law and the protection of privacy

The guiding statement of Article 17 has been observed by a number of European Court of Human Rights (ECtHR) decisions. The ECtHR's decisions in *Botta v Italy*[25], *MK v France*[26], *S and Marper v the UK*[27] and *Bensaid v the UK*[28] has suggested that 'private life is not an exhaustive decision.'[29] These decisions have shown the difficulty in a fully formed definition of privacy which includes all nuances that any individual might consider private. However, the ECtHR has stated that the very 'protection of personal data is of fundamental importance to a person's enjoyment of respect for his or her personal data and family life.'[30]

The United Nations and the international community must also take into account the Court of Justice of the European Union (CJEU)`s decisions on privacy. The landmark decision on privacy came in *Schrems v Data Protection Commissioner.*[31] This case was based on a complaint against Facebook brought to the Irish Data Protection Commissioner (IDPC). In the

complaint Schrems, challenged the transfer of his data to the United States by Facebook in light of Facebook USA alleged involvement with the PRISM mass surveillance program.[32] The Court of Justice of the European Union (CJEU) made the Safe Harbor arrangement of collection and data transfer between EU and US invalid. Schrems complaint was based on EU data protection law, which does not allow data transfers to non-EU countries, unless the company transferring and storing the data can guarantee adequate protection. The Court found that there was not the adequate protection needed in line with the EU data protection law and deemed that the Safe Harbor agreement 'must be declared invalid.'[33] The Court also expressed that 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental rights guaranteed by Article 7 of the Charter of Fundamental Rights of the European Union.'[34]

In conjunction with Article 28 of the ICCPR the Human Rights Committee (HRC) was formed to investigate and monitor states implementations of rights including those pursuant to privacy.[35] The HRC issued a General Comment on Article 17 of the ICCPR embodied by European case law which clarifying concepts such as 'arbitrary interference' 'family' 'home' and 'correspondence'. Although it must be stated again that the ICCPR is unclear as to what is always intended by these 'general comments' and an overarching definition of privacy in the digital age.[36]

However, the General Comment does state how from a legal aspect the ICCPR should be able to have an interpretation to the right to privacy within the scope of international law. According to the HRC the term 'unlawful' as it appears in Article 17 set out that no one's privacy must be interfered with unless reasoned by law.[37]

The right to privacy is not only recognised in some of the most important international and regional human rights documents but they have also been recognised in almost every constitution in the world. States without written constitutions like the UK for example have extended privacy protection through jurisprudence, procedural rules and other protections. Furthermore privacy has become a common element in most states.[38] Although the right to privacy is not an absolute right and at times is infringed when other matters are at stake (for example public protection or criminal sanction) there is a fine act of balancing the international community's inherent recognition of the right to privacy and the private act it may or may not protect.

There have also been several US cases which have influenced the international legal thinking on privacy protection. US courts have shown the approach of a balancing of the action taken by the user in determining whether the action is deemed private and obscure. In *United States v Gines-Perez*[39] the Court held that a right to claim privacy is unavailable to a person if they place information on a public forum without taken any steps to protect the information from discovery from the general public. In contrast in *Pietrylo v Hillstone Restaurant Group*[40] and an employee set up a private closed network page on Myspace with invitation only to join. The group was used mainly to convey frustration with their employer. When one of the managers obtained the password to the account, the creator of the group brought a case against the manager for an invasion of privacy. The Court held in favour of the infringement of privacy on the grounds that the group had been intended to be private and obscured from public view as it was by invitation only and each member had its own username and password.

It is not a secret that in certain circumstances states and their governments use surveillance and data collection within their borders of their own territories. However, this does raise the question as to whether they can carry out such acts in foreign states.

The ICCPR sets out in Article 2(1) 'states must respect and to ensure' the rights recognised in the treaty 'to all individuals within its territory and subject to its jurisdiction.'[41] The question of subject of under their jurisdiction raises questions of whom is under a state's jurisdiction. Global surveillance within different states and different legal frameworks makes a clear distinction between external and internal communications. Most states (namely the Five Eyes[42]) have legislation which governs these actions. In the UK it is the Regulation of Investigatory Powers Act 2000 (RIPA)[43], in the US it is the US Foreign Intelligence Surveillance Act 1978[44], Australian Intelligence Services Act[45] and Canadian National Defence Act 1985.[46]

For the UK under ss.8(1) and (2) of the RIPA internal communications and surveillance data gathering is only permitted when a warrant is issued and only on evidence of suspicion of unlawful activity.[47] External communications are defined as communication sent or received outside the territory of the British Islands.[48]

The invasion of privacy, which is in contrast with the ICCPR, is that the conditions of evidence and warrant set out s.8 (1) and (2) do not apply to external communications. This controversial element, is that all activities of UK residents through digital communications platforms such as Google, Twitter and Facebook, can be intercepted by the UK governmental state agencies as their headquarters are outside a British territory, in this instance the United States.[49] This therefore, gives the UK government through its intelligence gathering agencies permission to use all these communications which are coming in and out of the UK by UK residents. Another caveat to this is that under a general warrant under s. 8(4) RIPA 2000 both residents of the UK and foreign nationals can have their communications monitored.

The controversial nature of this was commented on by the HRC in a 2015 report in which it commented the following[50]:

> Regulation of Investigatory Powers Act 2000 (RIPA) that makes a distinction between internal and external communications, provides for untargeted warrants for the interception of external private communications and communication data, which are sent or received outside the United Kingdom without affording the same safeguards as in the case of interception of internal communications….the UK must review the regime regulating the interception of personal communications and retention of communication data with the view to ensuring that such activities both within and outside the State party, conform to its obligations under the International Covenant of Civil and Political Rights including Article 17.[51]

However, despite this request from the United Nations, the UK made no concession on this point. The Investigatory Powers Act 2016 under s 136(3) still allows for surveillance by their security forces to issue mass warrants to intercept 'overseas related communications.'[52]

Many states seem to absolve themselves from the obligations placed on them by ICCPR. The US government has refuted the obligation placed on it by ICCPR stating it is not bound by it.

The US ratified the ICCPR in 1992. Therefore, the US concludes that it is not legally bound to comply with ICCPR in respect to any surveillance operations over non-US communications systems or activities which are not based within the US. This position asserts that the US states that the ICCPR obligations are restricted to very specific circumstances. These circumstances

are when an individual is both within a state's territory and subject to its jurisdiction. Therefore, if these two conditions are not satisfied, it can be suggested, that the foreign individual concerned does not benefit from privacy protection under the ICCPR.[53]

In the UK, the Investigatory Powers Tribunal (IPT) has looked at the issue of the UK's international law obligations and human rights protections of individual privacy in *Human Rights Watch v Secretary of State*.[54] The Court here was concerned with the interception, storage and use of information and communications by the Government Communications Headquarters (GCHQ). The case concerned a group of UK residents and a group of individuals that were not residing in the UK. Regarding the question of the rights to privacy for the individuals not residing in the UK the court expressed that 'under Article 8 of the [European Convention on Human Rights (ECHR)] the UK owes no obligation to persons who are situated outside its territory in respect of electronic communications between them which passes through the state.'[55]

The IPT when investigating, therefore, considered two issues in relation to infringement of privacy. The first issue of standing (whether such an individual could make a claim from being directly affected) the tribunal decided that all the applicants had standing if they could provide the information necessary for the investigation. The controversial element was the second issue of extraterritorial application of the ECHR. The Tribunal concluded that the ECHR was not applicable to individuals living abroad even if they have been the subject to surveillance by the state.

Extraterritorial application concerns the issue of whether the ECHR applies to individuals abroad and whether states owe human rights protection to those individuals living outside their territory.[56] This discussion is concerned with the interpretation of the term 'jurisdiction' within the ECHR. The IPT therefore was submitting the question that is an individual under the jurisdiction of the UK if they have been under surveillance by the state but the individual is not domiciled within the UK.

The controversial issue of extraterritorial application decision by the IPT strikes at the very center of the right to privacy. Communications via the digital medium do not have respect for national borders and neither do digital communication companies or state government. Logic would suggest that the right to privacy should not be depended on an individual's location and whether they are protected by article 8 of the ECHR or under the ICCPR. The findings in *Human Rights Watch v Secretary of State* have been controversial and have been heavily criticized.[57]

International law must protect privacy by looking at the obligations on who is controlling individual communications not the effective control over physical areas or physical individuals. Nyst[58] argues that instead of looking at control as in physical control of territory, it must be looked at in terms of when data or communications are intercepted within that states territory, the state in question should be bound by rights obligations to those individuals regardless of their location. Nyst makes a suggestion that this is an 'interface-based jurisdiction,' that a state is not allowed to 'interfere with communications that passes through its territorial borders.'[59]

The bigger picture here is not just about the protected right of interference of communication and storing of data, but there is also the issue of collusion and the sharing of personal data between states which makes the obligation and protection of privacy so difficult to police against. The agreements between the US and other states allows governments to simply engage in the notion of 'collusion for circumvention.'[60] GCHQ is allowed to essentially spy on anyone

except British nationals[61] and the NSA through the PRISM surveillance program is allowed to spy on anyone that is not American.[62]

The PRISM program allows the NSA to collect communication from US internet communications companies. The collection of this data is governed by Section 702 FISA Amendments Act 2008 which allows communication data, encrypted data and search entries from companies such as Google, Yahoo and Microsoft to be transferred to the NSA.[63]

The documents leaked by Edward Snowden suggested that PRISM is 'the number one source of raw intelligence area for the NSA analytic reports and makes up approximately 91% of NSA internet acquired data.[64] The US government has defended the use of PRISM stating that is can only be used on US nationals with a warrant and it has prevented acts of Terrorism.[65]

Then the data information collected by GCHQ and the NSA is shared between the two agencies and therefore enables each agency to circumvent any national restrictions that are in place protecting its own citizens right to privacy, as they are able to access this information that has been gathered on their own citizens by foreign governmental agencies.[66]

International law and the future of privacy

The international community has taken steps to look at enhancing the protection of privacy since the adoption of the ICCPR in 1966 and the subsequent HRC's adoption of General Comment No 16 on the right to privacy in 1988.[67] These steps do include a focus on human rights and surveillance practices of the UN High Commissioner for Human Rights and the UN Special Rapporteurs on Freedom of Expression and Counter-Terrorism. The adoption of both UN General Assembly Resolutions and the UN Human Rights Council Resolutions on the right to privacy showed a focus on the issues by the international community. The 2015 creation of a UN Special Rapporteur on the Right to Privacy shows the focus on international importance of privacy. The HRC has also addressed surveillance legislation in its Concluding Observations to States. Also, the ECtHR, the CJEU and the Inter-American Commission and Court on Human Rights have developed a jurisprudence on right to privacy.

Of course there is a strong argument that these steps are not progressive enough. Most of these advancements can be seen as mainly regional agreements or soft law without any real binding obligations on states for the protection of privacy.

However, some of these wider international community discussions and advancements in the need to protect privacy have started to influence the legal framework of states intrusion into an individual's privacy. Canada's decision to stop the sharing of intelligence data with its Five Eyes partners was in direct response to the evidence of the unlawful surveillance of Canadians.[68] In 2014 the German Parliamentary Committee investigating the spy scandal involving the National Security Agency (NSA) has led to a lessening of the cooperation between the Federal Intelligence Agency (BND) and the NSA.[69] Also, there has been an increase in privacy cases in the German Courts.[70]

There has also been the proposition of more progressive data protection laws in the US. There have been two main proposals, consisting of the Consumer Online Privacy Rights Act (COPRA) and United States Consumer Data Privacy Act of 2019 (CDPA). This legislation would give the individual the right to sue private companies if they feel that their privacy rights

had been infringed. There have also been a number of proposals at federal level, including Online Privacy Act, Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data (DASHBOARD), American Data Dissemination Act (ADD Act), Social Media Privacy Protection and Consumer Rights Act of 2019 and the Privacy Bill of Rights Act.[71]

The UN has reaffirmed its commitment to the question of the protection of data in the digital age in Human Rights Council Resolution adopted in 2017 which reaffirmed its commitment to the issue by reaffirming many privacy issues that had previously been decided.

In 2015 via Resolution 28/16 the UN Human Rights Council decided to appoint after international community interest in the OHCHR Report into privacy a Special Rapporteur on the right to privacy for a period of three years.[72] The resolution directed the Special Rapporteur to report on alleged violations of the right to privacy including, in particular the concerns arising from new technologies. With this mandate in mind all member states were urged to cooperate fully with the office of the Special Rapporteur.

The main findings from the Special Rapporteur can be seen in the Report of the Special Rapporteur on the right to privacy from 27 February 2019.[73] In the report the Special Rapporteur states that the 'right to privacy can facilitate the enjoyment of other human rights. Equally its infringements constrain the enjoyment of other human rights.'[74] The report is critical of the states not taking seriously the regulations on privacy that they have signed up to stating: 'there are several historical examples of Member States ratifying international instruments on human rights while lacking the genuine will to take the necessary measures for their implementation.'[75] An example is former German Democratic Republic who signed the ICCPR in 1973 but was still openly using a surveillance regime against its citizens. The report went on to state that today there were similar contradictions. Many states commit themselves to protecting the right to privacy but are also acting in ways which puts the very protection of privacy at risk.[76]

The report used a Sieghart quote to explain that the right to privacy is integral to personal autonomy, the links between privacy, information flows, autonomy and power exist.[77] Sieghart suggests the following:

> 'In a society where modern information technology is developing fast, many others may be able to find out how we act. And that, in turn, may reduce our freedom to act as we please – because once others discover how we act, they may think that it is in their interest, or in the interest of society, or even in our own interest to dissuade us, discourage us, or even stopping us from doing what we want to do, and seek to manipulate us to do what they want to do.'[78]

The above position the Special Rapporteur linked to privacy in the following way[79]:

> 'Shorn of the cloak of privacy that protects him, an individual becomes transparent and therefore manipulable. A manipulable individual is at the mercy of those who control the information held about him, and his freedom, which is often relative at best, shrinks in direct proportion to the extent of the nature of the options and alternatives which are left open to him by those who control the information.'[80]

The report therefore clearly sets out the importance of the protection of privacy and it states 'infringing upon privacy is often part of a system which threatens other liberties.'[81] The report also reaffirmed the position of the HRC`s resolution of March 2017[82] that 'States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality.'[83]

The main privacy recommendations of the report included the following[84]:

> 47. The incorporation by UN Member States into their domestic legal system of the standards and safeguards set out in Convention 108+ Article 11[85], for the protection of the fundamental right to privacy, especially:
>
> (a) the creation of legal certainty by ensuring that any and all privacy-intrusive measures.
> (b) the establishment of the test of "a necessary and proportionate measure in a democratic society".
> (c) the establishment of one or more independent oversight authorities empowered by law and adequately resourced by the State.
>
> 48. (a) All UN Member States should amend their laws to empower their independent authorities entrusted with oversight of intelligence activities, to specifically and explicitly, oversight of all personal information exchanged between the intelligence agencies of the countries for which they are responsible.

The Special Rapporteur again expressed the importance of the right to privacy for individuals within the international community:

> 102. The confidence of individuals to share ideas and to assemble is also fundamental to the health of societies and democracy. The loss of privacy can lead to a loss of this confidence including confidence in Government and institutions established to represent the public interests, withdrawal from participation, which can adversely impact and undermine representative democracies.
>
> 103. While privacy rights are not costless, or free of risks to governments, the challenges are outweighed by our collective interest in democracy. The right to privacy for women, as well as children and individuals of diverse sexual orientations, gender identities, gender expressions and sex characteristics, is critically important for all of the reasons outlined above and reported in submissions.
>
> 108. Transparency is needed in how private companies use personal data of users, and respond to reports of online harassment. Greater gender diversity among those shaping online experiences is important for making products and platforms safer, more socially-responsible and accountable. [86]

Therefore, throughout, the findings of the Special Rapporteur and specifically the recommendations and conclusions from the report that the right to privacy is an area which needs the cooperation of states within the UN to insure that individual`s privacy or the obscurity of certain information is a protected right.

Conclusion

Individuals place a great deal of importance on the notion or essence of individual privacy. There is an inherent right of the individual to protect one's personal and private thoughts and actions. What an individual considers to be private is a question of interpretation. There is also a very real link between the need for privacy and the connection to dignity as human beings.

The need to protect this right is something which is becoming increasingly important and increasingly difficult within the digital age. The difficulty comes in the fact that much of our protected privacy is now within the digital sphere, making the protection from surveillance and intrusion from the state and private communications companies much harder to regulate.

The very general right to privacy can be recognised as the following:

> 'Privacy is a fundamental human right that has been defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others and free from state intervention and free from excessive unsolicited intervention by other uninvited individuals.'[87]

The evidence that the right to privacy is now considered to be within the higher scope of international law can be seen by its protected status within several international law doctrines and within international customary law.

The legal definition of a right to privacy needs to be a continuous and fluid process. The development and advances of new technology means that this area needs to be constantly adaptable to change. These developments will constantly make the application and protection of the need of an individual's privacy much more complex. As technology advances the temptation of states to use the technology to gather individual data becomes greater.

The current legal framework in international law is at times unclear. The UN through the Special Rapporteur is clear in reinforcing the rights protected under the ICCPR, UDHR, HRC`s General Comment no 17 and others but states are, especially through the Five-Eye states infringing individual rights, collecting data on individuals and using such data without permission.

However, complex the notion of privacy is, a fundamental right to be left alone or the right to obscurity, even though difficult, it is the responsibility of the law itself and in particular international law in protecting the individual and their privacy from interference by private companies and the state.

ENDNOTES

[1] Universal Declaration of Human Rights, 10 December 1948, GA/Res/217A

[2] International Covenant on Civil and Political Rights, 23 March 1976, 999 UNTS 171, Art. 17.

[3] United Nations Human Rights Council, *Report by the Special Rapporteur on the promotion and protection of the right to freedom and protection of the right to freedom of opinion and expression*, 2013, UN Doc., A/HRC/23/40.

[4] Human Rights Council, *UN Resolution on the Right to Privacy in the Digital Age*, 2017, UN Doc., A/HRC/RES/34/7.
[5] There are under international law two distinct control tests, one over territory and one over persons. The effective control test is based on acts of private individuals or groups controlled by the state. From *Nicaragua v United States*, ICJ Rep.14, (1986), 115.
[6] The often referred to Five Eyes comprises the US National Security Agency, the UK General Communication Headquarters, Canada's Communications Security Establishment, New Zealand's Government Communications Security Bureau and the Australian Signals Intelligence Directorate.
[7] United Nations Human Rights Commission, *General Comment No 16 Article 17 (Right to Privacy), The Right to Respect of Privacy, Family Home and Correspondence and Protection of Honour and Reputation*, 8 April 1988, UN Doc., HRI/GEN/Rev9.
[8] United Nations Human Rights Council, *Report by the Special Rapporteur on the promotion and protection of the right to freedom and protection of the right to freedom of opinion and expression*, 2013, UN Doc., A/HRC/23/40
[9] United Nations Human Rights Commission *General Comment No 16 Article 17 (Right to Privacy), The Right to Respect of Privacy, Family Home and Correspondence and Protection of Honour and Reputation*, 8 April 1988, UN Doc., HRI/GEN/Rev9
[10] Ibid., para 10.
[11] United Nations Human Rights Council, *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations in Spain*, 2009, UN Doc., CCPR/C/ESP/CO/5, para 11.
[12] Robert C. Post, 'Three Concepts of Privacy', *Georgetown Law Journal* 89 (2001): 2087.
[13] Alexandra Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace', *Groningen Journal of International Law* 2(2) (2014): 38.
[14] T. Gerety, 'Redefining Privacy' *Harvard Civil Rights-Civil Liberties Law Review* 12 (1977): 236 and William Parent 'Privacy Morality and the Law' *Philosophy and Public Affairs* 12 (1983) 4: 323.
[15] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1970) 330.
[16] Hyman Gross 'The Concept of Privacy', *New York University Law Review* 42 (1967) 1: 34-35.
[17] Daniel J. Solove *Understanding Privacy* (Cambridge: Harvard University Press, 2009) 13.
[18] Ibid., 39. Political scientist Priscilla Regan states that privacy interests are not individual interests but the interests of society. She explains that individual perceptions fail to appreciate the importance of privacy for individuals fails to recognise its importance as common, public and collective values. See Priscilla Regan *Legislating Privacy: Technology, Social Values and Public Policy* (Chapter Hill: University of North Carolina Press, 1995).
[19] P.B. Newell 'Perspectives on Privacy' *Journal of Environmental Psychology* 15 (1995)2: 88-105.
[20] Woodrow Hartzog and Fred Strutzman *'The Case for Online Obscurity'*, California Law Review 101 (2013): 1.
[21] Ibid., 112.
[22] Ibid., 113.
[23] *Ibid*.
[24] *Ibid*.
[25] *Botta v Italy, ECHR,* Appl. No 21439/93, (1994).
[26] *MK v France*, ECHR, Appl. No 19522/09, (2013).
[27] *S and Marper v UK*, ECHR, Appl. No 30542/04, (2008).
[28] *Bensaid v UK,* ECHR, Appl. No 44599/98, (2001).
[29] *S and Marper v UK*, ECHR, Appl. No 30542/04, (2008),para 47.

[30] *Botta v Italy, ECHR,* Appl. No 21439/93, (1994).
[31] *Maximilan Schrems v Data Protection Commissioner,* CJEU*,* C-362/14, (2015).
[32] PRISM is a code name for a mass surveillance program which the US National Security Agency (NSA) collects internet communications from various US based companies.
[33] *Maximilan Schrems v Data Protection Commissioner,* CJEU*,* C-362/14, (2015) para 92.
[34] Ibid., para 94.
[35] Article 28 International Covenant on Civil and Political Rights 1966.
[36] General Assembly Report of the Human Rights Committee 43rd Session, 1988, A/43/40.
[37] Ibid, para 3.
[38] Alexandra Rengel, *Privacy in the 21st Century* (Leiden: Martinus Nijhof Publishers, 2013).
[39] *United States v Gines-Perez*, D.P.R., F Suppl. 214 (2002) 205.
[40] *Pietrylo v Hillstone Restaurant Group,* D.N.J, WL 6085437 (2008).
[41] International Covenant on Civil and Political Rights, March 23 1976, 999 UNTS 171, Art. 17, Art. 2(1).
[42] Five Eyes comprises the US National Security Agency, the UK General Communication Headquarters, Canada's Communications Security Establishment, New Zealand's Government Communications Security Bureau and the Australian Signals Intelligence Directorate.
[43] United Kingdom, Regulation of Investigatory Powers Act, 2000, Sec., 8(4) and Investigatory Powers Act, 2016.
[44] United States, Foreign Intelligence Surveillance Act, 1978. Sec., 1881a(a).
[45] Australia, Australian Intelligence Services Act, 2001, Sec., 9.
[46] Canada, Canadian National Defence Act, 1985, Sec., 273.64(1).
[47] United Kingdom, Regulation of Investigatory Powers Act, 2000, Sec., 8(2).
[48] Ibid., Sec., 20.
[49] *Privacy International v GCHQ*, IPT/13/92/CH (16 May, 2014).
[50] United Nations Human Rights Council, *Concluding Observations on the Seventh Periodic Repost of the UK and Northern Ireland*, 17 August 2015, UN Doc., CCPR/C/GBR/Co/7.
[51] Ibid., 31
[52] United kingdom, Investigatory Powers Act, 2016, Sec. 136(3).
[53] United Nations Human Rights Commission, *Summary Record*, 1405th Meeting, 24 April, 1995, UN Doc., CCPR/C/SR 1405, para 20. United States Department, *Second and Third Periodic Report of the USA to the UN Committee on Human Rights Concerning the International Covenant on Civil and Political Rights*, 21 October, 2005.
[54] *Human Rights Watch Inc and Others v The Secretary of State for the Foreign and Commonwealth Office and Others,* ALL ER, (2016) 105.
[55] Ibid., 106.
[56] Marko Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (Oxford: Oxford University Press, 2011) 8.
[57] Scarlet Kim, 'ECHR Jurisdiction and Mass Surveillance: Scrutinising the UK Investigatory Power Tribunal's Recent Ruling', *EJIL:Talk!,* (June 9, 2016).
[58] Carly Nyst, 'Interface Based Jurisdiction Over Violations of the Right to Privacy', *EJIL:Talk!,* (November 16, 2013).
[59] Ibid., 48.
[60] Parliamentary Assembly of the Council of Europe 'Mass Surveillance', Doc. 13734, 2015, para. 30-33.
[61] Allowed to spy on British nationals only with reasonable suspicion.
[62] Parliamentary Assembly of the Council of Europe 'Mass Surveillance', para. 53.
[63] The Washington Post, 'NSA slides explain the PRSIM data collection program', *The Washington Post*, June 6, 2013.

[64] Glen Greenwald, 'NSA taps into internet giants' systems to mine data', *The Guardian*, June 6, 2013.
[65] Stepeh Ovide, 'US officials releases details of PRISM Program' *Wall Street Journal*, June 8, 2013.
[66] Ibid., 53.
[67] Human Rights Committee, General Comment 16, 22nd session, 21 UN Doc. HRI/GEN/1/Rev.1, (1988) 21.
[68] Associated Foreign Press, 'Canada Spy Agency Stops Sharing Intelligence with International Partners', *The Guardian*, January 28, 2016.
[69] The Guardian, 'German court backs murder's right to be forgotten online', *The Guardian*, November 27, 2019.
[70] *Ibid*.
[71] Dominic Rushe, 'Democrats propose sweeping new online privacy law to rein in tech giants,' *The Guardian*, November 26, 2019.
[72] The Special Rapporteur is mandated by Human Rights Council Resolution 28/16 to submit an annual report to the Human Rights Council and the General Assembly on information, trends, obstacles and violations related to the right to privacy.
[73] United Nations, *Report of the Special Rapporteur on the right to privacy*, February 27, 2019, Unedited Version, A/HRC/40/63.
[74] Ibid., para. 4.
[75] Ibid., para. 5.
[76] Ibid., para. 6.
[77] Ibid., para. 8.
[78] Peter Sieghart, *Privacy and Computers* (London: Latimer, 1976) 24.
[79] United Nations, *Report of the Special Rapporteur on the right to privacy*, February 27, 2019, Unedited Version, A/HRC/40/63, para. 9.
[80] Joseph Cannataci, *Privacy & Data Protection Law* (Oslo: Norwegian University Press, 1987) 60.
[81] United Nations, *Report of the Special Rapporteur on the right to privacy*, 27 February, 2019, Unedited Version, A/HRC/40/63, para. 10.
[82] Ibid., para. 2.
[83] Ibid., para. 17.
[84] Ibid., para. 46,47 and 48.
[85] Convention 108+ Article 11 is a Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No 108.
[86] United Nations, *Report of the Special Rapporteur on the right to privacy*, 27 February, 2019, Unedited Version, A/HRC/40/63, para. 102, 103 and 108.
[87] Martin Scheinin, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', *UN Human Rights Council*, (October 28, 2009): A-HRC-13-37.