International law, surveillance and the protection of privacy

Kristian P Humble

Received 27 Jan 2020, Accepted 25 Apr 2020, Published 15 May 2020

http://doi.org/10.1080/13642987.2020.1763315

Notes on the contributor

Kristian P Humble is a Principal Lecturer in International Law at the School of Law and Criminology at the University of Greenwich, London, UK, where he is the Programme Leader for LLB Programme. Kristian has taught undergraduate and postgraduate modules in human rights, international law and international criminal law. His research focuses on best practice in legal education, social justice, human rights and international law.

Abstract

The right to privacy is a fundamental human right under international law. The right to privacy for an individual is the right to hide or obscure elements of their life from the wider public. In the modern age the need for privacy is becoming increasingly difficult in light of modern communication companies which seek to make once which was considered private, public. The right to privacy has historically not been at the forefront of discussions within the international community and the United Nations. This position changed after the Edward Snowden and Cambridge Analytica revelations. The focus from the international community is on addressing not only the practices of state sponsored surveillance but also surveillance undertaken by modern communications companies. This article will focus on how the United Nations, the international community and international law aim to bring surveillance practices in line with human rights law and what privacy means in the modern digital age. The first part of the article will look at the inherent right to privacy, the second part will cover the recent developments from the United Nations and international law and the third part will look at the challenges ahead in the modern age of surveillance and digital communication.

Key words: Privacy, International Law, Rights, United Nations, Surveillance, State.

1. Introduction

The right to privacy is seen as a fundamental human right contained in the Universal Declaration of Human Rights (UDHR)[1] and the International Covenant on Civil and Political Rights (ICCPR).[2] The right to privacy however has historically not been at the forefront of discussions within the international community and the United Nations. This position

changed in 2013 after the Edward Snowden revelations. The international community was focused on addressing not only on the practices of state sponsored surveillance but also surveillance undertaken by modern communications companies.[3]

The basis of the international community and the United Nations in particular was the application and interpretation of Article 17 of the ICCPR and more recently the United Nations Resolution of Privacy in the Digital Age[4] and how to bring surveillance practices in line with human rights law and what is privacy means in the modern digital age.

The modern international law jurisprudence holds states accountable for their actions (not in all cases) based on the effective control test.[5] There has also been a suggestion of a different approach which is based on virtual control within the legal boundaries of holding states accountable over there surveillance activities while upholding the individual's right to privacy over their own communications.[6]

Recent events such as 2013 Edward Snowden and 2018 Cambridge Analytica revelations has shown that there needs to be an international legal solution to communication surveillance by states sometimes referred to as the Five Eyes[7] states and by communication-based companies such as Facebook. Activities which use surveillance without an individual's permission is in clear breach of Article 17 of the ICCPR. Despite the exposure of such practices (Snowden and Cambridge Analytica in particular) there has been a slow process of an agreement of how to bring these practices in line with international human rights law.

This article will deal with some of these challenges. The first part of the article will look at inherent right to privacy, the second part will cover the recent developments from the United Nations and international law, the third part will look at the challenges ahead in the modern age of surveillance and digital communication.

2. The meaning of privacy

The international community has been slow in responding to changes in technologies which are based on communication and data collection, leaving international law trying to catch up and regulate a growing concern for the protection of privacy of states and the individual.

Article 12 of the UDHR 1948 states the following:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the ICCPR 1966 states 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.[8] 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.

The ICCPR was in 1966 was not equipped to look at the threat to individual privacy from data collection and digital technologies because these technologies simply did not exist. Therefore, the definition of privacy is regarded as narrow in today's technological advances in communication and data collection. The 1988 General Comment only goes further to distinguish the incoming threat of data collection by states and the protection of states from individual's private data being interfered with. Again, however, a full appreciation of technologies concerning communication and information were not fully understood as the use of these technologies and the internet were in their infancy.

The way individuals communicate and the collection of data by states and technology companies seems to be commonly understood as being part of the digital age. But there needs to be discussion to look again at the General Comment from 1988 and an update for this new decade and beyond. The discussion was enhanced[9]by the United Nations Special Rapporteur Frank La Rue[10] and by the General Assembly.[11] The reason for an update is clear, there needs to be a fundamental understanding of what the right to privacy means and what it must

protect in light of the obligations of not only states but the more difficult notion of companies under international law.

The current General Comment to Article 17[12] 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.'[13] Also it can be seen that this has been agreed upon by the Human Rights Committee (HRC)[14] and this guiding statement of Article 17 has been followed in a number of European Court of Human Rights (ECtHR) decisions.

This guiding statement of Article 17 has been followed in a number of European Court of Human Rights (ECtHR) decisions. Indeed, the United Nations and the international community can take note of the ECtHR's decision in *Botta v Italy*[15], *MK v France*[16], *S and Marper v the UK*[17] and *Bensaid v the UK*[18] that the notion of 'private life is not an exhaustive decision.'[19] The court, therefore, does not feel that a definition on what is a private life can ever be fully comprehensive and include all aspects that an individual might feel are private. The ECtHR also 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.'[20]

The United Nations and the international community therefore should also take into account the Court of Justice of the European Union (CJEU)`s decisions on this matter. A landmark decision came in *Schrems v Data Protection Commissioner.*[21] This is seen as one of the most important international privacy cases in recent history. The 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.[22] 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.'[23] The Court also expressed that 'legislation permitting the public authorities to have access on a generalized 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.'[24]

2.1. Is there a right to obscurity in the digital age?

Privacy is an essential human need and an essential fundamental human right. The difficulty comes that the term privacy itself can be an abstract concept which at times is difficulty to define but all humans need the knowledge to know that elements of their private lives will be private and kept from others.

With the rise of new technologies, it is difficult to know where this fundamental right to privacy extends or even exists. With the internet and social media, it has become almost impossible to protect these fundamental rights and almost impossible for an individual to become invisible and keep themselves completely private.

Under the modern framework of international law, the protection of privacy for individuals depends entirely on constitutional limitations and states willingness to be adhere to international legal treaties and by bound by them. International law has however benefited from international custom as a source of law which means that the practice of certain types of actions will be enough to be recognised as binding on state parties. Article 38 of the International Court of Justice (ICJ)[25] Statute lists the sources of law in this regard and specifically sets out the importance of customary international law.[26] Customary international law has the status of law because the ICJ considers custom as 'evidence of a general practice accepted by law' and therefore 'part of the corpus of general international law'.[27] International customary law has at its core decision making value through state practice which can then evolve into a legal norm through consistent usage and then a final stage that this custom is accepted by the international community.[28] This is seen as a unique passage of law making within international law itself that the recognition of a custom or right can be enforced internationally without the express written agreement and consent of the sovereign power.

Therefore, to paraphrase the UDHR, a human right is based on an idea that there exists within the international sphere that a universal standard of rights which should be held in higher regard to local and cultural customs which are essential for dignity of human life.[29]

The need for privacy is seen in all cultures and civilisations, a need as humans that certain types or actions are of a private nature and should be away from general observation. Clarity to what the actions are and what constitutes privacy has and is a difficult subject to define.

Post suggested that:

> 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.[30]

This inherent need for privacy is also coupled with some sort of expectation that the state that one resides in will protect their privacy. The protection of this privacy will be from unwanted observation from other members of the public and from the state itself.

From Solove concept of privacy, in order to determine the action or behaviour that might cause an infringement of privacy and what level of protection might be needed it would be paramount to what the understood term of privacy meant. There would also need to be a distinction between the right to privacy and the concept of privacy.[31]

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.[32]

Therefore, it is impossible to formulate an argument for the obscurity in cyberspace without having a definition firstly of what constitutes privacy and secondly what then should be legally protected as a privacy issue for individuals.

As this article has suggested privacy has consistently been defined in the context of personal autonomy or having the innate control over the personal intimacies of personal identify or having control over the personal data which is available about yourself.[33] Many definitions of privacy vary from one element of privacy to another but what is clear is that privacy at its core is about the protection of oneself from the outside world.

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'[34] 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.'[35]

Solove has put privacy into six different concepts or general types based on his research:

(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.[36]

These categories are on the face of it common sense approaches to privacy matters that most individuals would agree that on some level all human beings need a level of the right to be left alone, secrecy, control or personhood. However, the problem exists in that some individuals will value some privacy matters 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 and private sometimes intimate images of oneself. So, the intrinsic problem lies in the notion that an overall definition of privacy may at times be out of reach or have to be contended on a more personal level.

Solove's own definition of privacy is that:

> 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.[37]

Therefore, Solove is also here looking at contextualising privacy, privacy which needs to change with time and maybe what privacy means to individuals and not the wider world interpretation of it. What an individual might hold dear in the scope of privacy might be very different to how another individual wants their privacy protected.

Privacy as most would ascertain is a general right to be left alone, for an amount of secrecy, to keep from the outside world aspects of oneself that an individual want or needs to keep private. As Newell explains privacy can be then 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.[38]

Another viewpoint here is that the right to privacy is wrapped up in the notion of self-worth and these notions by the very fact of their existence means that society itself can function more efficiently and in turn can proceed with purpose when these rights are protected. Regan suggest that 'I argue that society is better off…. when privacy exists. I maintain that privacy serves not just individual interests but common, public and collective purposes'.[39] Reiman suggests that 'privacy functions as a means of protecting freedom, moral personality and a rich and critical inner life.'[40]

The right to privacy of course has long been recognised in the international community. There are several (spoken addressed in this article) international conventions and human rights treaties which mention privacy as a central issue. In conjunction with Article 28 of the ICCPR the HRC was formed which investigates or 'monitors' states implementations of rights including those pursuant to privacy.[41] The HRC issued a General Comment on Article 17 of the ICCPR (also discussed in this article) which embodies the right to privacy, discussing and 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.[42]

The General Comment does however look at the legal aspect to how 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.[43]

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.[44] Although the right to privacy is not an absolute right and at times is infringed when other matters are at stake (like in light of public protection or criminal sanction) there must be 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.

The right to privacy includes the very idea that even though 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. But in cyberspace this is a very different and difficult concept to ascertain. 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.[45] Obscurity can be described as a 'state of unknowing or being unidentifiable online'.[46] Out in the public space it is impossible for an observer to identify someone identity or personal data because they do not have the correct pieces of this puzzle to fit together as they do not have access to any personal information. For instance 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.

Online obscurity is more complex but a person can remain obscure if a piece of vital personal information is missing like identity or social connections. But 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 simply the observing a conversation taken place in public.

Obscurity 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 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.[47] They have suggested that the protection of obscurity may be easier to implement than that of privacy recognition due in the main to the problematic nature of a widely accepted definition of a right to privacy. Obscurity they suggest could form a compromise remedy of protection. This would mean in essence instead of mandating that websites to remove sensitive information, the courts could propose some element of obscurity. So, companies storing personal information would have to keep the information online as it had been received, therefore if the individual did not want it to be exposed then it would not be exposed.

Hartzog and Strutzman suggested framework however does bring with it a number of other problems in which the individual in the protection information may not be initially satisfied with. This again still puts the individual information received and what to do with it in the hands of the receiving company, the trusting 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)[48]

Hartzog and Strutzman suggested the following as guidance:

> The presence of these factors diminishes obscurity, and their absence enhances it. Thus, in determining whether information is obscure online, courts should consider whether any of these factors were present in their determination. Information that is entirely unobscured is completely obvious, and vice versa. Like in fair use disputes, courts should engage in a case-by-case analysis of the factors, examining each one individually, then as a whole to determine the degree of online obscurity.[49]

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.[50]

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 user posts their name, a picture of themselves online in which they are easily identifiable then this cannot be a case of privacy and the individual cannot be assumed to have been trying to be obscure. If however elements within these four factors are missing as in the scenarios above then the court could determine that there was an element of obscurity intended to be observed.

There have been several US cases which the court has shown 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*[51] 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*[52] 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.

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 clearer.

3. Privacy protection under international law

It is understood that in certain circumstances states and their governments carry out surveillance and data collection within the borders of their own territories. However, this does raise the question as to whether they can carry out such acts in foreign states.

The scope of the ICCPR is clearly set out in Article 2(1) and sets out the following 'states must respect and to ensure' the rights recognised in the treaty 'to all individuals within its territory and subject to its jurisdiction.'[53] The question of subject of under their jurisdiction raises questions of whom is under a state's jurisdiction. Does this include individuals that are not within the territory of state?

However, global surveillance within different states and different legal frameworks makes a clear distinction between external and internal communications. Most states (namely the Five Eyes[54]) have legislation which governs these actions. In the UK it is the Regulation of Investigatory Powers Act 2000 (RIPA)[55], in the United States of America (USA or US) it is the US Foreign Intelligence Surveillance Act 1978[56], Australian Intelligence Services Act[57] and Canadian National Defence Act 1985.[58] These legislative frameworks show the obligations of protection of nationals and those within the state's territory and non-nationals who are living outside states territory.

For the UK under ss.8(1) and (2) of the RIPA communications which are internal may only be used in surveillance when a warrant is issued and only on evidence of suspicion of unlawful activity.[59] External communications are defined as communication sent or received outside the territory of the British Islands.[60]

This problematic element which contrasts with ICCPR and Comment No 16 is that the conditions of evidence and warrant set out ss.8 (1) and (2) do not apply to external communications. This controversial element here is that the UK governments would seem to suggest that all activities of UK residents through digital communications platforms such as

Google, Twitter and Facebook as their headquarters can be under surveillance as their data is held outside a British territory in the United States.[61]

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 using companies such as Google, Twitter and Facebook. 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[62]:

> 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.[63]

However, despite this request from the United Nations the UK made no concession on this point. In the new 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.'[64] So again just reconfirming the infringement of an individual's right to privacy protection as the RIPA 2000 does and on the face of it contrary to the ICCPR Article 17.

The concern is that the issue by individual states and information in the digital age is unclear. It is unclear on the extent to which information is being used by state agencies on the permission from governments. Many states seem to fragrantly 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 them. The US ratified the ICCPR in accordance with actions occurring outside its territory in 1992. Therefore, the US asserts 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 housed in 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 then the foreign individual concerned does not benefit from privacy protection under the ICCPR.[65]

In the UK state surveillance, the Investigatory Powers Tribunal (IPT) has looked at the issue of the UK's international law obligations and human rights protections of individuals privacy in the *Human Rights Watch v Secretary of State*.[66] The Court here was concerned with the interception, storage and use of information and communications by the Governement

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.'[67] 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.[68] The 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 is 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.

The findings in *Human Rights Watch v Secretary of State* have been controversial and have been criticized.[69] As the IPT decisions cannot be subject to a direct appeal in the UK, therefore, the IPT decisions could be challenged by the ECtHR.

3.1. ICCPR: Effective Control v Virtual Control

If states are primarily basing the jurisdiction of privacy on territorial this would seem to not fit easily with the circumstances which are set out within international law. However, all human rights courts and bodies, such as the International Court of Justice (ICJ) and the HRC, the Inter-American Commission on Human Rights (IACHR) that privacy issues may exist beyond merely a state's territory and exist outside a state's territory i.e. extraterritorially.

This simply put means a state is therefore bound by international law in relation in individuals who may not be domiciled within the state borders but who under the control of its jurisdiction. The HRC has adopted the following approach (similar to effective control) to determine not only the jurisdiction but also the protection of an individual's privacy where they are not domiciled within the state in questions borders:

> A state party must respect and ensure the rights laid down in the International Covenant on Civil and Political Rights to anyone within the power or effective control of that State Party even if not situated within the territory of the State Party.[70]

The IACHR established similar principles:

> The inquiry turns not on the presumed victim's nationality or presence within a particular geographical area but on whether under specific circumstances the State observed the rights of a person subject to its authority and control.[71]

How international law obligations may apply outside a state's geographical territory is spilt into two different categories: spatial and personal models. The spatial model sees jurisdiction as effective overall control over a specific geographical area, but the personal model sees it as a physical control over the individual in question.

The spatial model was established in the ECtHR case *Loizidou v Turkey*. In this case the Court established 'a state's responsibility was engaged when as a consequence of lawful or unlawful military action it exercised effective control of an area outside its national territory.'[72] In the International Court of Justice case *DRC v Uganda* it was held that the ICCPR applies 'extraterritorially when a state is occupying territory of another state.'[73]

However, both these examples seem to apply to military exposition and control but do not go far enough in everyday protection of individuals right to privacy. Milanovic stated that in some circumstances during conflict states could control areas without being in another state's territory. For example, the use by a state of drones during conflict would have effective control over an area without physically being in another states territory.[74]

The case of *Lopez Burgos v Uruguay*[75] is important to note here, even though not directly about privacy it is important in the context of effective control of individuals and whether they should have the same protection of their rights regardless of where they are domiciled. In this case the applicant was alleged to have been kidnapped and tortured in Argentina by Uruguayan security and intelligence forces due to his trade union activities, despite having a visa to enter Austria and having political refugee statues granted by the UNHCR. The HRC emphasized in this case that an individual right and the protection of them do not diminish once they are domiciled in a foreign state. The HRC expressed these obligations in the following way:

> It would be unconscionable to so interpret the responsibility under Article 2 of the ICCPR 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…a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party even if not situated within the territory of the State Party…regardless of the circumstances in which such power or effective control was obtained.[76]

Therefore, a state must have under international law a human rights obligation by the means of the effective control over an individual. In times of conflict this rule would need to be extended to encompass the obligation of a state where there is the privacy of communications by an individual who is residing in a foreign state.

The effective control test works well in times of conflict due to the physical nature of the definition and the finding of international courts but is harder to make it fit with modern privacy concerns over surveillance and interception of individual's private communications.

Margulies[77] has suggested that the existing effective control test is 'inadequate for the cyber and communications realm as it places the emphasis on the exercise of physical over persons or territory which is difficult to relate to cyberspace.'[78] Therefore, Margulies suggested that the US which has unprecedented virtual power and the narrowly defined standard of privacy requiring physical control means that it is easy to exploit this gap by ignoring their human rights obligations. The US for example has relationships with communications companies allowing direct access to surveillance transmitting devices, undersea cables and other carriers of internet and telephonic communications.[79]

Then international law must protect privacy by looking at the obligations in the controlling of communications not the effective control over physical areas or physical individuals. Nyst[80] 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 owe obligations to those individuals regardless of their location on the basis Nyst suggests of 'interface-based jurisdiction' that a state is not allowed to 'interfere with communications that passes through its territorial borders.'[81]

Nyst has the same thinking of Milanovic[82] who distinguishes between the positive obligation of states to protect human rights and to preventing human rights violations by third parties and negative obligation of states to respect human rights that only require states to refrain from interfering with the rights of individuals without sufficient justification.[83] Milanovic therefore is suggesting that within this construct it sees jurisdiction as a negative duty to not interfere and therefore all violations as negative when interfering with privacy.[84]

Both Nyst and Milanovic approaches here look at the weakness of the privacy debate couched in the confines of the personal and spatial models and put at the center of their thinking that there must be an emphasis on the negative duty that states cannot interfere with rights that are protected.

There is also a larger picture here which is not just about the protected right of interference of communication and storing of data. There is also the subject 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.'[85] GCHQ is allowed to essentially spy on anyone except British nationals[86] and the NSA through the PRISM surveillance program is allowed to spy on anyone that is not American.[87]

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.[88]

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.[89] 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 act of Terrorism.[90]

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.[91]

There has also been a suggestion of the 'virtual control test'. This was proposed by Margulies[92] who suggested that a virtual control test would make the ICCPR and other international human rights treaties applicable when a state can assert 'virtual control' over an individual's communications even if the state does not have control over the territory the individual is located.[93] Margulies suggests that virtual control would mean when a state intercepts, stores and analyses an individual's communications.

Of course, this test is a suggestion and has not be accepted or adopted by the international community as the expansion or different approach to privacy and the protection of it. Paust has criticised the approach as it has little or no shared legal expectation about personal jurisdiction and privacy.[94]

However, such an approach does not fit with the jurisprudence of the ECtHR in the case of *Jaloud v Netherlands*.[95] For example, in this case the court took a more expansive approach and extraterritorial jurisdiction in privacy matters was suggested, because the state can 'exercise authority and control over individuals right to life which made the physical nature of effective control unimportant.'[96]

A virtual control test would ensure equal treatment of all individuals not dependent on their location because the establishing a virtual control test would not depend on where the communications took place but rather on whether a state can have control of it even if its lacks control over the territory or physical person.

The HRC has addressed this matter head on suggesting extraterritorial surveillance does not affect the right to privacy and the ICCPR. The HRC suggested:

> The Committee is concerned about the surveillance of communications in the interest of protecting national security conducted by the National Security Agency (NSA) conducted both within and outside the United States.[97]

United Nations Office of the High Commissioner also addressed the issue:

> Digital surveillance may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found for example through direct tapping or penetration of that infrastructure. Equally where a State exercises regulatory jurisdiction over a third party that physically controls the data that State also would have obligations under the Covenant.[98]

The Special Rapporteur observed:

> State's jurisdiction is not only engaged where State agents place data interceptors on fibre-optic cables travelling through their jurisdictions but also where a State exercises regulatory authority over the telecommunications or Internet service providers that physically control the data.[99]

The UN General Assembly when adopting Resolution 68/167 expressed:

> At the negative impact that surveillance including extraterritorial surveillance in particular when carried out on a mass scale may have on the exercise and enjoyment of human rights.[100]

Therefore, it can be seen that a virtual control test is needed as the elements which make up the effective control test over privacy do not fit the digital age. It is impossible to know where and how physical control is made in the traditional sense and where in the traditional sense territorial control is ascertained. This is because with digital communications, all such communications are sent through various different territories and jurisdictions before the reach their destination of the user. So, what becomes important, is whether the control virtual can be implemented regardless of where the individual is located or their nationality.

All these viewpoints look to a need for the international community and the UN to look again at the Article 17 of the ICCPR and issue a new Comment stipulating the protection of privacy in the digital age.

3.2. United Nations and the future of surveillance

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.[101] 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.

There are of course the arguments (as this article has already suggested) that these steps are not progressive enough. Most of these advancements are merely regional agreements or soft law principles without much real binding force on states and their behaviour towards the right to privacy.

However, some of these advancements have started to influence the behaviour of states towards the intrusion of states into 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.[102] 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.[103] Also, there has been an increase in privacy cases being decided by German Courts.[104]

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.[105] The resolution directed the Special Rapporteur to report on alleged violations of the right to privacy including in particular 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 right to privacy report; Report of the Special Rapporteur on the right to privacy from 27 February 2019.[106] 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.'[107] He is also 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.'[108] The example used 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 this privacy at risk.[109]

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.[110] 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.[111]

The above position the Special Rapporteur linked to privacy in the following way[112]:

> 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.[113]

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.'[114] The report also reaffirmed the position of the HRC`s resolution of March 2017[115] that 'States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality.'[116]

The main privacy recommendations of the report included the following[117]:

> 47. The incorporation by UN Member States into their domestic legal system of the standards and safeguards set out in Convention 108+ Article 11[118], 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.

In conclusion[119] 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.

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 protection and the cooperation of states within the UN to insure that individual`s privacy or the obscurity of certain information is a protected right.

4. Cambridge Analytica and the right to privacy

This part of this article will focus on the way forward for the right to privacy after the Cambridge Analytica scandal and how this may be a focus for reevaluation of the what is privacy and who should hold the key to private information of individuals. Whether this is the inherent right to privacy which is incumbent in international treaties or the right to obscurity in cyberspace one element is clear and that there is a need for tightening up of the law in this area to be clear for those companies that hold individual's information on what will constitute a breach and punishment for the misuse of personal data.

On March 17 2018, the New York Times and the Guardian published stories exposing that the personal data of over 50 million Facebook users were in the possession of a company called Cambridge Analytica.[120] Cambridge Analytica was a company[121] which had links not only to the 2016 US election but also the 2016 UK Brexit Referendum.[122]

Cambridge Analytica was a British political data consulting firm which combined data mining, data brokerage and data analysis with strategic communication which used specifically during election campaigns.[123] The personal data of up to 87 million Facebook users were acquired via the 270,000 Facebook users who used an app called 'This is Your Digital Life'. By giving this third party app permission to acquire data (in 2015) this also gave the app access to information which was stored on the apps user's associate networks Therefore this resulted in data of about 87 million users, the vast majority of who had not given Cambridge Analytica the permission to access their personal data.[124]

Cambridge Analytica were based on a system engineered by Michal Kosinski. The system was based around a profiling system of general online data from likes on Facebook and data collected from smartphones. Kosinski suggested that with a limited number of 'likes' individuals can be analysed more efficiently and individual psychological targeting is a powerful tool to influence people.[125] Cambridge Analytica would then collect data on potential voters using this data via such actions as demographics, consumer behaviour and internet activity. According to The Guardian, the data used psychological data derived from millions of Facebook users without permission.[126] Other sources of information included the 'Cruz Crew' which was a mobile app that tracked physical movements and contacts.[127]

The use and collection of personal data without permission raises privacy issues and ethical concerns. But Cambridge Analytica company base was in the United States and privacy laws are not enacted with protecting privacy. The Cruz Crew app's database has been described as "political-voter surveillance."[128]

Cambridge Analytica scope was wide and influence widespread. In India Cambridge Analytica was used by the Indian National Congress to carry out analysis of the electorate and influence voters in the 2010 elections. It was found that 355 Indian Facebook users had installed a Cambridge Analytica app which then in turn exposed the data of 562,455 other users. The Indian National Congress was also given data information by Cambridge Analytica for the 2019 general elections.[129] Cambridge Analytica ran secret campaigns in Kenya for the 2013 and 2017 elections.[130] There are also accusations that Cambridge Analytica had influence on elections in Australia, Malta and Mexico.[131]

However, by far the most controversial influence Cambridge Analytica had was alleged to have had was on the US 2016 Presidential elections and the 2016 EU Referendum in the UK is seen as the most controversial.

Cambridge Analytica became involved in the 2016 UK European Union Membership Referendum (commonly known as Brexit) using data to convince 'persuadable' voters to vote to leave the European Union.[132] Articles that appeared in February and May in 2017 in the

Observer and the Guardian suggested respectively that Cambridge Analytica had influenced the Vote Leave campaign and Donald Trump's 2016 presidential campaign.[133] It was claimed that Cambridge Analytica had produced a document claiming that it could affect the outcome of the referendum with the data it had collected. The document was entitled 'Big Data Solutions for the EU Referendum' and claimed it could single out vote leave voters, donors, politicians and journalists.[134]

In March 2018 Christopher Wylie a former Cambridge Analytica employee told the UK Electoral Commission that a firm linked to Cambridge Analytica helped the official Vote Leave campaign by circumventing the financing laws in place during the EU referendum.[135]

Cambridge Analytica involvement in the 2016 presidential primaries for the Republican Party became known in July 2015.[136] As of December that same year Cambridge Analytica claimed to have collected up to 5,000 data points on over 220 million US citizens.[137] After Ted Cruz dropped out of the Republican presidential nomination race, Cambridge Analytica started to work closely with Republican candidate Donald Trump.

On 18 May 2017 the US Congress started to investigate Cambridge Analytica in connection with possible Russian interference in the 2016 US election campaign.[138] It was suggested the Cambridge Analytica breached data privacy by spreading Russian propaganda using micro targeting.[139] In 2018 it was found that Cambridge Analytica had used 50 million Facebook users personal data without permission while assisting Donald Trump's presidential campaign. This information it was suggested was used to influence the US election in Donald Trump's favour.[140]

In the UK the Information Commissioners Office (ICO) conducted an investigation into data analytics for political purposes and in response to the Cambridge Analytica scandal obtained new and stronger powers as the UK Data Protection Act 2018. In November 2018 the ICO published its report to Parliament on the use of data in political campaigns and highlighted:

> A disturbing disregard for voters' personal privacy by players across the political campaigning system from data companies and data brokers to social media platforms, campaign groups and political parties.[141]

Mark Zuckerberg (CEO Facebook) announced in March 2019 that Facebook would build a 'privacy focused messaging and social networking platform.'[142] He was criticised for failing to address whether the company would stop purchasing information from data analysts, harvesting data from individuals not using Facebook.[143]

The importance of the discussion on Cambridge Analytica is its impact on the wider discussion on the protection of privacy. After the scandal broke it seems that the international community has been forced into action on the right to privacy and access to data issues. This has seen investigations in Italy Germany and Canada. These investigations have all led to the call on Facebook to regulate its use of personal data.

Within the discussions of this article, Cambridge Analytica and the focus it put on privacy does not seem to have influenced any enhancements in fundamental international legal protection of privacy. It seems that it has had a greater influence on regional discussion and region reform. If international law had a more robust approach to how privacy should be protected and more measures which are not on a voluntary basis, then international human rights law would and should be the basis of protection from the privacy breach seen by Cambridge Analytica and any future incarnation.

Therefore, without the necessary framework in place it would seem privacy protection from international law and the United Nations in the case of Cambridge Analytica would be difficult.

5. Future development of privacy protection under international law

There is data protection, as this article has set out in UDHR, ICCPR and an interpretation of data protection guaranteed by the UNHRC. The protection of privacy within international law is uncertain due to several competing factors.

International human rights treaties (like the ICCPR) do not mention the need for data protection specifically and the guidance and guarantees are very broad which leaves little room for direct guidance for the courts.

International legal framework is fragmented between international human rights law, regional legal agreement and national legal agreements. For example, there is a fundamental rights approach in EU law[144] in the protection of individual privacy contrasting with the US approach[145] based on a more consumer protection approach. As Kittichaisaree and Kuner state few states agree with position of the US that international law does not preclude unauthorized intelligence gathering as long as the activity does not involve commercial or industrial espionage or the destruction of data.[146]

A future development of protection under international law could take three main areas of privacy rights protection.

Firstly, there is a need for a more precise normative framework based on what is privacy and obscurity for the courts or a new legal framework to address. This could be based on Hartzog and Strutman four factors for recognition of what is private and what is public privacy as discussed early in this article.[147]

Secondly, to draft a new international agreement dealing with data protection. This would have the profound advantage of setting out a clear, precise framework based around privacy protection. However, there are obstacles to such an agreement. An agreement between all states on what is privacy and the need to balance the need of data protection for the individual

against the wider needs of society. For example, states would still uphold the right of infringement of privacy in light of terrorism concerns. There might also be the practical barrier that a treaty-based solution might not provide the most adequate remedy in an area which is as fast moving as data protection and future technologies.

Thirdly, international law could accept that data protection is too fragmented to have one centralised hierarchical system of protection. Kittichaisaree and Kuner suggest that this would allow data protection to develop on a regional and national level though international cooperation, therefore allowing privacy protection that could develop over time that states could adopt voluntarily at a national level providing a common internationalised approach to the protection of privacy.[148]

It is clear what is needed is a holistic approach from the international community which brings together implementation of data protection laws at a national level which could then influence a more progressive development of the protection of individual privacy at an international level.

6. Conclusion

Individuals place a great deal of importance on the notion of privacy. There is an inherent right of the individual to protect one's personal and private thoughts and actions. The right to protect privacy is important in establishing and forming human relationships. There is also a very real link between the need for privacy and the connection to dignity as human beings.

As this article has shown at the international level there is evidence through treaty level implementation to the continuing discussion at the UN level that privacy and the existence of privacy is a fundamental right which exists as a universal principle of human existence. 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 much harder to regulate.

The 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.[149]

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. Of course, there is a cavate to this which is prevalent within the international law sphere that this right to privacy is not an absolute right and in most cases this right is balanced against the interest of states.

The legal definition of a right to privacy needs to be a continuous 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 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.

Privacy and its protection are a complex notion and there are not any failsafe routes to individual privacy protection. There is a fundamental right to be left alone and elements of this article has discussed whether an individual has a right to obscurity in the digital age. This article shows there are positive steps being made in the international community for the protection of individual privacy. However, the one thing is clear is that the law and international law in particular must be clearer and more robust to protect the individual from interference from the state and private companies.

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] United Nations General Assembly, *Report of the Office of the United Nations High Commissioner for Human Rights; the Right to Privacy in the Digital Age*, 2014, UN Doc., A/HRC/27/37, para 20.

[7] 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.

[8] 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.
[9] Notably from the Human Rights Committee (HRC).
[10] 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
[11] United Nations General Assembly, 18 December 2013, Res 68/167 UN Doc., A/RES/68/167, United Nations General Assembly, 18 December 2014, Res 69/166 18, UN Doc., A/RES/69/166.
[12] 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
[13] Ibid., para 10.
[14] 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.
[15] *Botta v Italy, ECHR,* Appl. No 21439/93, (1994).
[16] *MK v France*, ECHR, Appl. No 19522/09, (2013).
[17] *S and Marper v UK*, ECHR, Appl. No 30542/04, (2008).
[18] *Bensaid v UK,* ECHR*,* Appl. No 44599/98, (2001).
[19] *S and Marper v UK*, ECHR, Appl. No 30542/04, (2008),para 47.
[20] *Botta v Italy, ECHR,* Appl. No 21439/93, (1994).
[21] *Maximilan Schrems v Data Protection Commissioner,* CJEU*,* C-362/14, (2015).
[22] 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.
[23] *Maximilan Schrems v Data Protection Commissioner,* CJEU*,* C-362/14, (2015) para 92.
[24] Ibid., para 94.
[25] Statute of the International Court of Justice, 26 June 1945, 33 UNTS, 993.
[26] See above, Article 38, (1)(b).
[27] *North Sea Continental Shelf Cases, ICJ,* Reports 3, 28, (1969).
[28] Philip Alston, *Human Rights Law* (New York: New York University Press, 1996) 3-8.
[29] Unite Nations General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217A, (III).
[30] Robert C. Post, 'Three Concepts of Privacy', *Georgetown Law Journal* 89 (2001): 2087.
[31] Daniel J. Solove, 'Conceptualizing Privacy' *California Law Review* vol 90 (2002) 4: 1087.
[32] Alexandra Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace', *Groningen Journal of International Law* 2(2) (2014): 38.
[33] 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.
[34] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1970) 330.
[35] Hyman Gross 'The Concept of Privacy', *New York University Law Review* 42 (1967) 1: 34-35.
[36] Daniel J. Solove *Understanding Privacy* (Cambridge: Harvard University Press, 2009) 13.
[37] 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).
[38] P.B. Newell 'Perspectives on Privacy' *Journal of Environmental Psychology* 15 (1995)2: 88-105.
[39] Priscilla Regan *Legislating Privacy: Technology, Social Values and Public Policy* (Chapter Hill: University of North Carolina Press, 1995).
[40] Jeffrey H. Reiman '*Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future'*, Santa Clara High Tech Law Journal 11 (1995)1: 27.
[41] Article 28 International Covenant on Civil and Political Rights 1966.
[42] General Assembly Report of the Human Rights Committee 43rd Session, 1988, A/43/40.
[43] Ibid, para 3.
[44] Alexandra Rengel, *Privacy in the 21st Century* (Leiden: Martinus Nijhof Publishers, 2013).
[45] Woodrow Hartzog and Fred Strutzman *'The Case for Online Obscurity'*, California Law Review 101 (2013): 1.
[46] Ibid., 112.
[47] Ibid., 113.
[48] *Ibid*.
[49] Ibid., 36
[50] *Ibid*.
[51] *United States v Gines-Perez*, D.P.R., F Suppl. 214 (2002) 205.
[52] *Pietrylo v Hillstone Restaurant Group,* D.N.J, WL 6085437 (2008).
[53] International Covenant on Civil and Political Rights, March 23 1976, 999 UNTS 171, Art. 17, Art. 2(1).
[54] 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.
[55] United Kingdom, Regulation of Investigatory Powers Act, 2000, Sec., 8(4) and Investigatory Powers Act, 2016.
[56] United States, Foreign Intelligence Surveillance Act, 1978. Sec., 1881a(a).
[57] Australia, Australian Intelligence Services Act, 2001, Sec., 9.
[58] Canada, Canadian National Defence Act, 1985, Sec., 273.64(1).
[59] United Kingdom, Regulation of Investigatory Powers Act, 2000, Sec., 8(2).
[60] Ibid., Sec., 20.
[61] *Privacy International v GCHQ*, IPT/13/92/CH (16 May, 2014).
[62] 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.
[63] Ibid., 31
[64] United kingdom, Investigatory Powers Act, 2016, Sec. 136(3).
[65] 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.
[66] *Human Rights Watch Inc and Others v The Secretary of State for the Foreign and Commonwealth Office and Others,* ALL ER, (2016) 105.
[67] Ibid., 106.
[68] Marko Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (Oxford: Oxford University Press, 2011) 8.

[69] Scarlet Kim, 'ECHR Jurisdiction and Mass Surveillance: Scrutinising the UK Investigatory Power Tribunal's Recent Ruling', *EJIL:Talk!,* (June 9, 2016).
[70] United Nations Human Rights Commission, *General Comment No 31 The Nature of the General Obligations Imposed on State Parties to the Covenant*, 2004, UN Doc. CCPR/C/21/Rev.1/Add1326, para 10.
[71] *Alexandre v Cuba*, IACHR, Case 11.589, Report No 109/99, (1999) para 37.
[72] *Loizidou v Turkey,* EHRR, 20, (1995) 98.
[73] *Case Concerning Armed Activities on the Territory of the Congo in Democratic Republic of Congo v Uganda,* ICJ, (2000) 111.
[74] Marko Milanovic 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', *Harvard International Law Journal*, 81 (2015):113.
[75] *Lopez Burgos v Uruguay*, Communications No 52, UN Doc., CCPR/C13/D/52/1979, (1979).
[76] Ibid., para 10.
[77] Peter Margulies, 'The NSA in the Global Perspective: Surveillance, Human Rights and International Counterterrorism' *Fordham Law Review* 82 (2014): 2137.
[78] Ibid., 2150.
[79] *Ibid*.
[80] Carly Nyst, 'Interface Based Jurisdiction Over Violations of the Right to Privacy', *EJIL:Talk!,* (November 16, 2013).
[81] Ibid., 48.
[82] Ibid., 126.
[83] Ibid., 50.
[84] Ibid., 129.
[85] Parliamentary Assembly of the Council of Europe 'Mass Surveillance', Doc. 13734, 2015, para. 30-33.
[86] Allowed to spy on British nationals only with reasonable suspicion.
[87] Parliamentary Assembly of the Council of Europe 'Mass Surveillance', para. 53.
[88] The Washington Post, 'NSA slides explain the PRSIM data collection program', *The Washington Post*, June 6, 2013.
[89] Glen Greenwald, 'NSA taps into internet giants' systems to mine data', *The Guardian*, June 6, 2013.
[90] Stepeh Ovide, 'US officials releases details of PRISM Program' *Wall Street Journal*, June 8, 2013.
[91] Ibid., 53.
[92] Peter Margulies, 'The NSA in the Global Perspective: Surveillance, Human Rights and International Counterterrorism', *Fordham Law Review* 82 (2014): 2139.
[93] Ibid., 2157.
[94] Jordan J. Paust, 'Can You Hear Me Now? Private Communications, National Security and the Human Rights Disconnect', *Chicago Journal of International Law*, 15 (2) (2015): 612.
[95] *Jaloud v Netherlands,* ECHR*,* Appl. No 47708/08, (2014).
[96] *Ibid*.
[97] United Nations Human Rights Council, 'Concluding Observations on the Fourth Periodic Report of the USA', April 23, 2014, CCRP/C/USA/CO/4, para. 22.
[98] Ibid., para 34.
[99] United Nations, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 2014, UN Doc. A/69/397, para. 41.
[100] United Nations General Assembly, Res 68/167, 18 December, 2013.

[101] Human Rights Committee, General Comment 16, 22nd session, 21 UN Doc. HRI/GEN/1/Rev.1, (1988) 21.
[102] Associated Foreign Press, 'Canada Spy Agency Stops Sharing Intelligence with International Partners', *The Guardian*, January 28, 2016.
[103] The Guardian, 'German court backs murder's right to be forgotten online', *The Guardian*, November 27, 2019.
[104] *Ibid*.
[105] 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.
[106] United Nations, *Report of the Special Rapporteur on the right to privacy*, February 27, 2019, Unedited Version, A/HRC/40/63.
[107] Ibid., para. 4.
[108] Ibid., para. 5.
[109] Ibid., para. 6.
[110] Ibid., para. 8.
[111] Peter Sieghart, *Privacy and Computers* (London: Latimer, 1976) 24.
[112] United Nations, *Report of the Special Rapporteur on the right to privacy*, February 27, 2019, Unedited Version, A/HRC/40/63, para. 9.
[113] Joseph Cannataci, *Privacy & Data Protection Law* (Oslo: Norwegian University Press, 1987) 60.
[114] United Nations, *Report of the Special Rapporteur on the right to privacy*, 27 February, 2019, Unedited Version, A/HRC/40/63, para. 10.
[115] Ibid., para. 2.
[116] Ibid., para. 17.
[117] Ibid., para. 46,47 and 48.
[118] 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.
[119] 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.
[120] There were a number of individuals who helped expose Cambridge Analytica; Carole Cadwalladr (journalist), Christopher Wylie (a former employee of Cambridge Analytica), Shahmir Sanni (a volunteer with the Vote Leave Campaign in the UK Brexit Referendum), and Professor David Carrol, a Professor, who has engaged in a lengthy battle to obtain his data from Cambridge Analytica.
[121] The company was partly owned Robert Mercer, an American hedge-fund manager who supports manly conservative political causes. The CEO was Alexander Nix. Nix has suggested has that Cambridge Analytica was involved in forty four US political races in 2014. In 2016, Cambridge Analytica worked for Donald Trump's presidential campaign as well as for Leave.EU. CA's role in those campaigns has been controversial and is the subject of ongoing criminal investigations in both UK and US. See David Hakim, 'Data Firm Says Secret Sauce Aided Trump; Many Scoff', *The New York Times*, October 28, 2018. Also see Carol Cadwalladr, 'Watchdog to launch inquiry into misuse of data in politics, *The Guardian*, October 29, 2019.
[122] Privacy International*, 'Guide to International Law and Surveillance', Privacy International,* https://privacyinternational.org/long-read/993/guide-international-law-and-surveillance-20 (accessed November 8, 2019).

[123] Editorial, 'Who is Cambridge Analytica and what did it do?', *Reuters*, https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F (accessed 10 November, 2019).
[124] Alex Hern, 'How to check whether Facebook shared your data with Cambridge Analytica', *The Guardian,* April 10, 2018.
[125] Kosinski, Stillwell and Graepel, 'Private traits and attributes are predictable from digital records of human behavior', *Proceedings of the National Academy of Sciences*, 110 (2013): 5805.
[126] Harry Davies, 'Ted Cruz using firm that harvested data on millions of unwitting Facebook users', *The Guardian,* https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data (accessed October 30, 2019).
[127] Michael Biesecker and Julie Bykowicz, 'Cruz app data collection helps campaign read minds of voters', *AP News*, https://apnews.com/2db0fc93cf664a63909e26e708e91c67/cruz-app-data-collection-helps-campaign-read-minds-voters (accessed October 30, 2019).
[128] *Ibid*.
[129] *Ibid*.
[130] Jina Moore, 'Cambridge Analytica had role in Kenyan election too', *New York Times*, https://www.nytimes.com/2018/03/20/world/africa/kenya-cambridge-analytica-election.html (accessed November 3, 2019).
[131] Channel 4 News, 'Data, Democracy and Dirty Tricks', *Channel 4 News*, https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose (November 10, 2019).
[132] The Guardian, 'Cambridge Analytica Files', *The Guardian*, https://www.theguardian.com/news/series/cambridge-analytica-files (accessed November 10, 2019).
[133] Carole Cadwalladr, 'The Great British Brexit robbery how our democracy was hijacked' *The Guardian,* https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy (accessed November 15, 2019).
[134] Joe Murphy, 'Cambridge Analytica bragged: We have vast data for Brexit vote", *London Evening Standard* https://www.standard.co.uk/news/uk/cambridge-analytica-bragged-we-have-vast-data-for-brexit-vote-a3797441.html (accessed November 13, 2019).
[135] Carole Cadwalladr, 'I made Steve Bannon's psychological warfare tool: meet the data war whistleblower', *The Guardian* https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (accessed January 18, 2020).
[136] Kenneth Vogel, 'Cruz partners with donor's 'psychographic' firm', *Politico*, https://www.politico.com/story/2015/07/ted-cruz-donor-for-data-119813 (accessed November 5, 2019).
[137] Carole Cadwalladr, 'I made Steve Bannon's psychological warfare tool: meet the data war whistleblower', *The Guardian* https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (accessed December 18, 2019).
[138] Massimo Calabresi, 'Inside Russia's Social Media War on America' *Time,* https://time.com/4783932/inside-russia-social-media-war-america/ (accessed November 18, 2019).
[139] *Ibid*.
[140] The Great Hack. Directed by Jehane Noujaim and Karim Amer. United States: Netflix.
[141] Privacy International, 'Cambridge Analytica, GDPR 1 year on a lot of words and some action', *Privacy International*, https://privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-lot-words-and-some-action (accessed November 3, 2019).

[142] Zeynep Tufekci, 'Zukerberg's So Called Shift Towards Privacy', in *New York Times*, https://www.nytimes.com/2019/03/07/opinion/zuckerberg-privacy-facebook.html (accessed 3 November, 2019).
[143] Roger McNamee, 'Mark Zuckerberg says he wants to fix the internet. Don't take him seriously' *The Guardian*, https://www.theguardian.com/commentisfree/2019/apr/02/mark-zuckerberg-fix-the-internet (January 26, 2020).
[144] EU Directive 95/46.
[145] Kriangsak Kittichaisaree and Christopher Kuner, 'The growing importance of data protection in public international law', *EJIL: Talk*, https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/ (accessed March 6, 2020).
[146] *Ibid*.
[147] Woodrow Hartzog and Fred Strutzman *'The Case for Online Obscurity'*, California Law Review 101 (2013): 1.
[148] Kriangsak Kittichaisaree and Christopher Kuner, 'The growing importance of data protection in public international law', *EJIL: Talk*, https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/ (accessed March 6, 2020).
[149] 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.