UNIVERSITY OF HELSINKI

The Erik Castren Institute of International Law and Human Rights

&

European Master's Degree in Human Rights and Democratisation

## E.MA Master's Thesis

# Adjusting the right to privacy to Virtual Reality: Example of copyright enforcement policies

written by

Paula Hakkaja

Supervisors: Alejandro Lorite Escorihuela & Magdalena Kmak

Second Semester University: University of Helsinki, Finland

Academic Year 2012/2013

Words: 27 642

12 July 2013

**ABSTRACT**

Every significant progress or shift in human history has been triggered by innovation – fire, wheel, electricity. The challenge of these discourses is the ways in which human species adopt to the changes. These technological changes also change the discourse of the society. Hence, if applying old behaviours to new challenges, no progress is encouraged. All of these shifts have taken place in the field of human interaction and knowledge. Either indirectly, such as fire and electricity; or directly, such as language and internet.

The shift that has been encouraged by the invention of internet is evident in the digital divide between generations and encouragement to create a new sphere of social life online. The online openness of internet generation is triggered by not having to adapt, as such, to the changes in their daily lives. The problems of privacy online different from offline, as the understanding of space and time is blurred and private versus public actions can take place simultaneously, such as in social networks. The philosophy of privacy comes in here. Firstly, the concerns, cases, frustrations over privacy issues mainly arise from social moral judgement. By creating a public sphere which does not have limits in space and time and opening up to that sphere, subjects individuals to increased judgements. The conscious voluntary act of sharing personal information is viewed as a problem only when the information cannot be erased and does not allow the ´forgetting´ but the being subjected to prejudice continues in present in terms of ´big data´. This awareness of being subjected to judgement creates extended sensitivity of individuals. Copyright viewed as an expression of private thoughts to encourage the exchange of information, knowledge and progress. This paper attempts to analyse the impact of cyberspace and copyright enforcement on human rights. The first chapter deals with the traditional approach to right to privacy as guaranteed by Article 8 of the European Convention on Human Rights. The second chapter identifies specific features of cyberspace and how it shapes the ways in which people experience life. Third chapter looks at how these changes of life experience that happen in online world, affect the reasonable expectation of privacy that individuals have. Final chapter focuses on

problematic areas in policies of copyright enforcement, which emphasises the need to adapt the right to privacy to characteristics of cyberspace.

**Table of Contents**

## CHAPTER 1

The right to privacy under the European Convention on Human Rights

### 1.1. Introduction.

Article 8 of the European Convention on Human Rights (ECHR) establishes the right to respect for private and family life. It provides that:

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

Firstly, article 8 consists of a ´negative´ obligation to interfere with one´s privacy (Art. 8(1)) and a ´positive´ obligation for the state to take steps in order to prevent interference with the rights of others (Art. 8(2)). In order to understand the application of the Convention, the terminology of it must be assessed. First part of this chapter will assess how the European Court of Human Rights (the Court) has interpreted the features of the convention. These include recognising that privacy is relative to public interaction and it must be distinguished. This is the base for the attempt to define what is private by the Court in various cases. Privacy has so many dimensions and one of the main questions this arises is: Do individuals have privacy in public places and to what extent? However, the right to privacy is not exclusive, as established by Article 8(2). It is important to distinguish the conditions, under which the interference is allowed, in order to protect the rights of others. This is analysed in part 1.4 of this chapter. It also looks at the state obligation to protect its people, but with a manner that does not cause arbitrary interference. Finally theoretical values of privacy, such as autonomy, identity and conscience, will be assessed.

1.2. Distinguishing private from public.

To establish the elements that are relevant when distinguishing between private and public, the Court referred to the case of *P.G. and J.H.*

*Since there are occasions when people knowingly or intentionally involve themselves in activities which are recorded in a public manner, a person's reasonable expectations as to privacy may be a significant factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain."*[1]

In this case, the police installed a covert listening device in the applicant´s flat for the purposes of crime prevention. The Court based its reasoning on the fact that no sufficient law regulating the listening devices existed at the time. Hence, the measures were not ´in accordance with law´. The second issue looked at was if the police obtaining information regarding the numbers dialled at a specific date was ´in accordance with law´. This was the result of the Telecommunications Act 1984 and the Data Protection Act 1984 providing a legitimate basis for the disclosure of billing information to public authorities. The second element of the Court´s assessment of ´prescribed by law´ also included the criteria for ´quality of law´ in terms of foreseeability. It concluded that it was not an issue because the information *´did not include any information about the contents of those calls, or who made or received them. The data obtained, and the use that could be made of them, were therefore strictly limited.´*[2] Despite the lack of sufficient regulation of storage and destruction of obtained information, the Court found the interference with privacy ´in accordance with law´, because it was not convinced that the *´ lack of such detailed formal regulation raises any risk of arbitrariness or misuse´.*[3] Furthermore, it was established that the interference was ´necessary in democratic society´ for the purpose of public safety and

[1] *P.G. and J.H.* v. the *United Kingdom*, no. 44787/98, 25 September 2009, ECHR 2001-IX, §57.
[2] *P.G. and J.H.* v. the *United Kingdom*, no. 44787/98, 25 September 2009, ECHR 2001-IX, §46.
[3] *Ibidem*, §47.

prevention of disorder and crime as provided under Article 8(2). The Court, hence, has taken a position where the systematic storage of data obtained in public can create an interference with the right to privacy. On the other hand, the perception that lack of regulation on storage of the data, from the private sphere (the phone bills of the applicant were not created in a public), does not create misuse puts the Court into the position where systematic private records do not interfere with the right to privacy. The interference would take place if the information included any details about the content. However, mere data gathering would not apply.

F. Schoeman describes the state of violation in situations of monitoring only if a certain norm is infringed.[4] Here the norm is set to the handling of the data. The systematic storage of data from public undermines the norm of right to privacy in public when it is related to individuality. For instance the level of privacy is lessened if the individual is part of the mass in the street and the mass as a whole is captured on a photograph. On the other hand if the recording of public data is linked to technology of recognition where the individual is systematically identified, then the concerns of privacy arise regardless of the space. In private space the norm is dependent on the processing of the information. Such as in the present case, the storage of pure data, without the storage of the content as such, is not an issue of privacy as it can be compared to the notion of public privacy. The mass of pure data can be considered comparable with general mass of the public, where no personal details are identified.

1.3. Public privacy.

Definition of ´privacy´ by the Court is not an exhaustive list. The case of *Peck* concerns the applicant, who was suffering from depression, went to the street (public space) with a knife in his hand and the intention to commit a suicide.[5] His behaviour was noticed by the CCTV (Closed-Circuit Television) operator who notified the police. The issue in the case was that the footage of the applicant was released in the press without consent or covering the face. In fact, the applicant found out, that he had been recorded and

[4] F. Schoeman, *Privacy: philosophical dimensions of the literature,* Philosophical Dimensions of Privacy: an Anthology, 1984, p. 4.
[5] *Peck v. the United Kingdom,* no. 44647/98, 28 January 2003, 36 EHRR 719.

published from his neighbours who saw him on television.[6] The Court pointed out features of ´private life´ that establish its approach to defining it.

*´Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Article 8. That Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".*[7]

In the case of *Peck,* there was legislation in place that regulates the powers of the police, such as Criminal Justice and Public Order Act 1994. The case of involves similar concerns as *P.G. and J.H,* such as gathering data through the CCTV monitoring. However, as the applicant *´ admitted that that function of the CCTV system, together with the consequent involvement of the police, may have saved his life´,* the concern was not related to obtaining or storage of data.[8] The point of concern was the disclosure of the *´record of his movements to the public in a manner in which he could never have foreseen which gave rise to such an interference´.* As the Local Government Act 1972 enabled Brentwood Borough Council to distribute the CCTV footage to the media, for the purposes of promoting the usage and effectiveness of the CCTV technology, the interference of the right was in accordance with law. In fact, the disclosure of the footage was titled in press as: ´Defused – The partnership between CCTV and the police prevents a potentially dangerous situation´.[9] The court reached a conclusion of violation of Article 8 as a result of assessment of proportionality based on three elements. Firstly, *´ the applicant was not charged with, much less convicted of, an offence,´* hence, it would dismiss the ´necessity´ claim based on the prevention of crime [10] Secondly, the aim of the disclosure of the footage, according to the Council, was to increase

[6] *Ibidem* §18.
[7] *Ibidem* §57.
[8] *Peck v. the United Kingdom,* no. 44647/98, 28 January 2003, 36 EHRR 719, §60.
[9] *Ibidem,* §13.
[10] *Ibidem,* §79.

transparency and ´ *inspire public confidence and support for the system and to deter criminals´.*[11] However, the means were not proportionate as the police should have asked for the consent of the individual prior to the disclosure of the data. Thirdly, the Court concluded that the failure to mask the identity of the applicant in the media amounted to disproportionate interference with his privacy.

*Peck* is one of the principal cases for establishing privacy in public. N.A. Moreham has related the public privacy to the will of an individual to be accessible to others.[12] Even in the public, an individual has a choice of the extent of the private information he or she reveals to the public around. The information can be transferred through behaviour; hence, there is certain behaviour that people practice in private only. The first issue here is the ´will´ to be exposed. For instance, in the case of *Peck*, could it be assumed that the claimant willingly denounced his right to privacy in public because he willingly exposed himself in public? Moreham justifies public privacy because of the voluntariness to exposure and the extent of it. For instance, even though the applicant in *Peck* was in public, he still had a choice of the extent of the public. He chose his behaviour and actions with a conscious understanding of his audience (the people and the cars on the street).[13] His lack of consent to be published becomes relevant as he was exposed, through press releases of the footage, to a different and larger group of audience that he anticipated. In *Peck* the Court said that *´the relevant moment was viewed to the extent which far exceeded any exposure to passer-by´* or which the claimant *´could have reasonably foreseen´*[14]. Therefore, the determinant of the public privacy becomes a ´reasonable expectation´ of it, which is itself dependent on the location of the individual the nature of his or her activity and the means in which the information was obtained.[15]

[11] *Ibidem*, §69.
[12] N.A. Moreham, *Privacy in public places*, The Cambridge Law Journal, 2006, p. 617.
[13] *Ibidem*, p. 618.
[14] *Peck v. the United Kingdom*, no. 44647/98, 28 January 2003, 36 EHRR 719, §62.
[15] , *N.A. Moreham, Privacy in public places*, The Cambridge Law Journal, 2006, p. 620.

1.4. Obligations of the state.

Both of these cases can be considered under the principle of ´negative´ obligation of the state to interfere with privacy. The principles that the Court must consider after establishing the interference is, firstly, the requirement for the interference to be in accordance with (national) law that is subjected to the rule of law. To be accordance with the law, the law itself must be accessible to the person and in accordance with the principles of foreseeability.[16] Rule of law entails that the relevant legislation must also *´provide a measure of legal protection against arbitrary interference by the public authorities with the rights safeguarded by Article 8(1).´*[17] Second requirement is that the legitimate aim is one of those outlined in Article 8(2). Finally, the court considers the principle of ´necessary in democratic society, ´ which means that there must be a pressing social need for the interference with the right.[18] In addition to the ´negative´ obligations, states are also under ´positive´ obligations that are *´inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.´*[19] In other words, states are under an obligation to provide legislation that protects individuals from arbitrary interventions by the state but also unjustified interference by private individuals.

Despite of the Courts defining ´private life´ as not an exhaustive list, Moreham has divided the meaning of ´privacy´ in five distinct categories that reflect the case law. The five categories are: 1) the freedom from interference with physical and psychological integrity; 2) the collection and disclosure of information; 3) protection of one´s living environment; 4) identity; and 5) personal autonomy.[20] The measures of all the categories are subjected to the principles of prescribed by law, legitimate aim and necessary in democratic society. However, for the purposes of this paper, the categories

[16] *Segerstedt-Wiberg v. Sweden,* no. 62332/00, 6 June 2006, 44EHRR 4, §76.
[17] *Ibidem.*
[18] *Dudgeon v. the United Kingdom,* no. 7525/76, 22 October 1981, 4 EHRR 149, § 51.
[19] *Van Kuck v. Germany,* no. 35968/97, 12 June 2003, 37 EHRR 51, §70.
[20] N.A. Moreham, *The right to respect for private life in the European Convention on Human Rights: a re-examination,* European Human Rights Law Review, 2008, pp. 49-71.

of Moreham are assessed in terms of what is proportionate to the aim pursued, hence, the necessary in democratic society principle.

The first category includes surveillance (unwanted listening or watching) and can be applied to the cases of *Peck* and *P.G. and J.H.* However, the point of collection and disclosure of information is only partially addressed in the case of *Peck* and it must be elaborated upon. As seen in *Peck*, the collection of data must be proportionate and not intrusive. However, the case of *Rotaru* establishes that recording and storing applicant´s political and criminal activities for more than fifty years falls under the scope of ´private life´.[21] Furthermore the Court *´recognises that intelligence services may legitimately exist in a democratic society, it reiterates that powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions´*.[22] Hence, for the purposes of preservation of democratic societies the principles of rule of law and foreseeability must apply. *´A rule is "foreseeable" if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct.´*[23] In regards to the third category of living environment, even though not explicitly stated in the Convention, the Court has stated that *´Article 8 may apply in environmental cases where the pollution is directly caused by the State or whether the State responsibility arises from the failure to properly regulate private industry.´*[24] Here the court has elaborated on the negative versus positive obligation. However, the right to environment is not expressly stated in the Convention and, yet, the Court has extended the meaning of the right to privacy. This opens doors for further expansion of the right when the Court faces new challenges that can be indirectly linked to privacy. This is an indication that the Court does not necessarily have to stick to specific limitations under Article 8(2), but can link anything unsaid to the ´protection of health or morals, or for the protection of the rights and freedoms of others´.[25] Whether the interference is manifested directly or through the failure to regulate, the Court has established a two-step assessment process. *´First, the*

[21] *Rotaru v. Romania,* no. 28341/95, 4 May 2000, 8 BHRC 449, ECHR, §44.
[22] *Ibidem,* §47.
[23] *Ibidem,* §55.
[24] *Hatton v. the United Kingdom,* no. 36022/97, 8 July 2006, 37 EHRR 28, §98.
[25] Ariticle 8(2), European Convention on Human Rights.

*Court may assess the substantive merits of the government's decision, to ensure that it is compatible with Article 8. Secondly, it may scrutinise the decision-making process to ensure that due weight has been accorded to the interests of the individual.´*[26] The fourth category of identity include *´information concerning highly personal aspects of applicant´s childhood, development and history.´*[27]It also includes gender identity[28] and cultural identity[29]. Moreham distinguishes the developing identities from the right to live autonomously.[30] Cases involving the right to establish relationships, sexual or of other nature, and the right to exercise control over one´s health are the only types of cases that fall under autonomy. Moreham notes that all interferences with private right are also interferences with autonomy.[31] However, autonomy, as established by this categorization, implies the freedom to choose as it is referred to as ´human freedom´. Firstly, the concern that arises from ´autonomy´ and ´human freedom´ is the ambiguity of the terms. As the Court is resistant in defining ´privacy´ exclusively, it cannot strictly identify autonomy merely with ´intimate´ choices, such as concerning sexual or medical choices.[32] The second issue is the danger that, with the progress and changes in the society and case law, the line between autonomy and identity blurs. Identity becomes highly dependent on autonomy for two reasons. Extensive intervention in ´human freedom´, outside of the court room, becomes an interference with the freedom to make autonomous choices of how to behave, which reflect back at identity. Furthermore, the ´development of identity´ cannot be separated from the identity itself. For example, sexuality as identity cannot be separated from living autonomously, which is the reference to forming intimate relationships.

[26] *Hatton v. the United Kingdom,* no. 36022/97, 8 July 2006, 37 EHRR 28, §99.
[27] *Gaskin v. the United Kingdom,* no. 10454/83, 7 July 1989, 12 EHRR 36, §36.
[28] *I v. the United Kingdom,* no. 25680/94, 11 July 2002, 36 EHRR 53.
[29] *Chapman v. the United Kingdom,* no. 27238/95, 8 January 2001, 33EHRR 18.
[30] N.A. Moreham, *The right to respect for private life in the European Convention on Human Rights: a re-examination,* Europan Human Rights Law Review, 2008, p. 71.
[31] *Ibidem.*
[32] Medical choices are often limited due to monopolization, intellectual property rights etc. The autonomy to choose is affected by the margin of appreciation.

1.5. Theoretical considerations of the right to privacy.

The understanding of value of privacy can only be achieved through the understanding of individual behaviour in public. Firstly, the notions of privacy have emerged due to the awareness that there is behaviour that does not gain its validity through social approval.[33] This is the awareness that gives rise to individual consciousness and autonomy to choose how to behave in certain space. It allows the individual consciously cohere with social norms and yet maintain his or her identity. Hence, privacy has been defined as a measure of control that an individual has over the information regarding him, intimacies of personal identity and who has access to the individual.[34] Individual autonomy and freedom of conscience are two interlinked features of what privacy is. Freedom of conscience is the basis for autonomy and the human freedom. It is the freedom of conscience that is the basis for autonomous decisions regarding the value and extent of privacy that one aims to achieve. F. Schoeman gives an example of a man on a lonely island, where, even though he has lost control over information about him, and yet, he still has too much privacy in solitude. The freedom of conscience is an element that allows individuals to decide when it is too much or too little privacy intuitively, regardless of how it is defined by law or social contracts. Furthermore, it allows the subjective value of privacy compared to other rights. The individual consciousness incorporates individual interests that mark the actions as autonomous. Autonomy becomes a primary concept of privacy as it allows an individual the right to choose when and by whom to be observed and, as a consequence, regulate his or her behaviour accordingly. In liberal-democratic societies, individual interests are considered to be closely linked to individuality, autonomy and also identity, and it is difficult to distinguish these notions from each other in privacy concerns. Hence, indirect interference with consciousness and autonomy can be found in all privacy cases. However, the biggest challenge is abstaining from interfering with consciousness directly by shaping the discourses of human behaviour that has emotional dimensions. James Fitzjames Stephen wrote in 1874 that privacy can be violated by compelling a

[33] F. Schoeman, *Privacy: philosophical dimensions of the literature,* Philosophical Dimensions of Privacy: an Anthology, 1984, p. 13.
[34] F. Schoeman, *Privacy: philosophical dimensions of the literature,* Philosophical Dimensions of Privacy: an Anthology, 1984, p. 2.

person to direct too much intention to his own feelings.[35] In addition, this is a theoretical indication of why the Court has put such great emphasis on privacy as the right to develop and maintain human relationships with an intention to abstain from interfering with such relationships. In fact, it has been suggested that the notion of intimacy would not exist without the right to privacy. [36] All mentioned above is highly linked to control and personal autonomy. The control can be seen as the extent of which the individual chooses to expose himself in public space or the extent that the individual, for whatever subjective reasons, decides that some matters should be private to escape public scrutiny. Daniel Solove criticizes conceptualizing privacy in terms of control because he claims that the definition of control in itself is too vague and broad.[37] He raises a valid point as conceptualizing privacy merely in terms of control does not allow the development of sufficient legislative framework for the protection of privacy. Furthermore, he claims that this conception is too narrow because it focuses too exclusively on individual autonomy.[38] However, he does not here account for the principle that liberalism is based on individual autonomy and democracy on the collective individualism where the people, despite of personal interest, collectively create a social standard for the amount of control they have over the state authorities. Hence, these two features must maintain one of the central focuses when speaking of privacy in liberal-democratic societies.

### 1.6. Conclusion

Privacy is always relative to its exposure to public intervention. The method that has been adopted to distinguish between private and public looks at the means of gathering data. For instance, surveillance requires legitimate procedures and purpose in order to be ´in accordance with law´. The cases of *P.G. and J.H* and *Peck* establish two ways in which privacy can be intervened with in public spaces. Firstly, private life considerations arise when permanent record of persons and their private characteristics come into existence. Secondly, even in public, individuals have reasonable expectation

[35] *Ibidem*, p. 11.
[36] R. S. Gerstein, *Intimacy and privacy*, Philosophical Dimensions of Privacy: an Anthology, 1984, p. 270.
[37] D. Solove, Understanding Privacy, 2008, p. 29.
[38] *Ibidem.*

of privacy. Reasonable expectation becomes the most valuable and significant feature when defining what is private and how it can be intervened in. Modern liberal democracies are based on individual autonomy. Autonomy will be undermined if privacy will not be considered according to the expectations of individuals. Of course, the freedom requires some form of responsibilities, but only if people know what is expected from them. However, technological developments, especially in the field of information and communication technology, change the distinction and definition of privacy.

## CHAPTER 2

Characteristics of cyberspace.

### 2.1. Introduction

Major progresses and shifts in human history has been triggered by new innovations, for example fire, wheel and electricity. All of the most significant discoveries have shifted the discourses of human interaction and knowledge. Either indirectly, such as fire and electricity; or directly, such as language and the internet. The challenge of these discourses is the ways in which human species adopt to these changes. Warren and Brandeis argue that advances of civilization have cultivated new sensitivities and vulnerabilities. The increasing complexity and intensity of life in general make an individual´s ability to retreat from the world crucial.[39] Behavioural science tells us how the changes also shape behaviours. Hence, if applying old behaviours to new challenges, no progress of the societies is encouraged. The shift that has been encouraged by the invention of the internet is evident in the digital divide between generations and encouragement to create a new sphere of public space online. In order to address the ways in which privacy right should or should not be enforced online, the parameters of social change in the era of internet must be defined. However, defining cyberspace can be as difficult and complex as defining what is privacy.

[39] F. Schoeman, *Privacy: philosophical dimensions of the literature*, Philosophical Dimensions of Privacy: an Anthology, 1984, p. 14.

APRANET, the ancestor of the internet, was set up in 1960 by the United States Government that served a military security purpose. Its goal was the creation of information network system that would survive a nuclear attack. The initial goal was further enhanced in 1990 when Tim Berners-Lee, who at the time was employed by the European Organisation for Nuclear Research (CERN), created a World Wide Web (WWW or the Web). The Web allowed browsing of shared information in a user-friendly means.[40] The increased user-friendliness means that it is easily accessible to be used by general public. As a result, the internet cannot be defined and assessed in pure technological terms.[41] The use and abuse of it is dependent on the human factor, rather than technological means. Purely technological approach regards internet as a static system, or at least with calculable projections of advancements and progress. The objectified human knowledge, new informational content, communication systems and global limitless access to information shape the parameters of internet separately from the technological advancements.[42] To understand how the cyberspace affects the established dimensions of privacy, it must be assessed in two different sub-categories. First, looking at cyberspace as a social, economic and public space; and secondly how the technological features affect the *´virtual´* space to become reality.

## 2.2. Features of cyberspace

Cyberspace can be described as social because it's a product of social processes. Christian Fuchs describes something as social when it is produced by humans in social relations and is used and applied in these social relations.[43] Hence, any advancement in the society, not only in terms of cyberspace, can be considered as a social product as it is dependent on human relationships. Any innovation is a result of human knowledge that is incorporated in a form of social act of gaining that knowledge. It does not necessarily have to be direct interaction with another human, but can be indirect through receiving information from books, for example. No individual or social progress can take place in complete isolation from the relevant context that the knowledge can be

[40] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 121.
[41] *Ibidem.*
[42] *Ibidem,* p. 122.
[43] *Ibidem,* p. 126.

applied in. In that light, it is important that social space is distinguished from public space. The distinction is relevant to the relative amount of privacy in each space. Cyberspace as a social space means that it is comparable to society as a whole, which incorporates public and private actions and thoughts. Public space implies a notion by an individual that he has given up some forms of privacy when entering the public. It does not have to be so in social space. Hence, cyberspace is not either public or private space, but another space as a whole for the society to exist in. The features that differentiate cyberspace from conventional social space are the relativity of public versus private and concept of time.

The first and most obvious feature of cyberspace is the fact that it changes the concept of space and time. When people are communicating through internet, they do not have to be in the same place. Firstly, two people can be thousands of miles apart and still communicate in the same time. The same applies to a telephone. However, what is different in cyberspace is that the communication does not anticipate an immediate and spontaneous response. In a chat or e-mail the response is in writing and, hence, allows more comprehensive response which actually does not take place in exact same time. Furthermore, the feature of experiencing space changes as one can access a virtual public space in a physical private space. The simplest example here is accessing a social networking cite while being alone in your private bedroom. In addition to the changes of conventional understanding of space, the conventional human experience of time changes along. Aristotle´s philosophy on the concept of time starts from the point of human observation of time. *´Where no change is perceived no time is perceived, for when the state of our own minds does not change at all, or we have not noticed its changing, we do not realise the time has elapsed.´*[44] Hence, the concept of time is a human realisation of change in surroundings. The same principles of time apply to cyberspace. However, when connecting to the Internet, one can get lost in time. When not paying attention to time, the realisation of elapsed time becomes difficult because one does not experience the changes is cyberspace in a physical space. The understanding of what is real depends on the experience of space and time. It is

[44] P. Conen, *Aristotle´s Definition of Time,* The New Scholasticism, 1952, p. 441.

common understanding that having dinner at a physical table with one´s family is a reality. However, can it then be assumed that dining and talking to a family over, for example video conversation on Skype, is not real? The experience of dining together, as such, still creates an experience of family dinner, which is real in spite of the changed notion of time and space. The cyberspace does not put an end to the notion of real space or time, but merely accelerates the social interactions to the global scale.[45] This brings us to the notion of *´virtual reality´*. Considering virtual reality is relevant when comparing the norms of reality to the social norms of cyberspace. Manuel Castells refers to this new social phenomenon as a *´culture of real virtuality´*.[46] It is virtual because of the technological means of communication and tangible means to create reality. However, it is real because *´it is our fundamental reality, the material basis on which we live our existence, construct our systems of representation, practice our work, link up with other people, retrieve information, form our opinions, act in politics, and nurture of our dreams.´*[47] The increased purpose, complexity and the rapid spread of the Internet usage, that turn cyberspace into real space, means that in its importance to human development it cannot be distinguished from *´real´* reality. However, if the virtual creation of space becomes real as we experience it, then the dilemma of how to regulate it arises. Even though it cannot be distinguished in the notion of reality, it must be distinguished how the society and legislation adopts to that shift of reality. Virtual reality can be divided into four sub-categories: social, economic, public and private reality. The argument that accessing cyberspace is voluntary or a choice is no more valid. Hence, the rationale of voluntary reassignment of privacy when entering a public space becomes out dated. Cyberspace is a new playground for life that cannot be escaped.

### 2.3. Social reality

The importance of social media in everyday lives of people cannot be ignored. The social reality in this section mainly consists of the right to form and maintain relationships. As the European Court of Human Rights has considered the right to form

[45] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 137.
[46] M. Castells, *The Internet Galaxy*, 2001, p. 203.
[47] *Ibidem.*

personal relationships a matter of privacy, it must be noted that the rise of social media is in itself a matter of private relationships. The figures of social media use speak for itself. As of March 2013 Facebook had 1.11 billion monthly active users.[48] Considering that 2,4 billion people in 2012 globally used the Internet then the number of Facebook users is nearly half[49]. This does not count for other social media sites, but illustrates the massive growth and importance of similar websites. This raises a question whether such a massive scale of social media usage makes it a public or merely a social space. If it is defined as a public space then any information that is disclosed by an individual would become voluntary exposure to public and privacy rules that apply to the public spaces as defined by the Court would apply. Therefore, only privacy would be protected only in certain matters if the intervention is exceeding the normal parameters of being seen by everyone in a public space. However, as the purpose of social media websites remains to be on the level of relationships. Facebook users accept friends with whom only they want to share certain information with. It marks the autonomy to whom one wants to expose certain aspects of their life. With the rise of social media, the users of the Internet have realised that the Internet is not anymore for the purposes of receiving information but also a place to share it. With social media each ´receiver can be a sender or information, each consumer a producer.´[50]

The effect of social websites on how people experience their (social) life is what makes it real. Several studies on the psychological impact of the Internet have been conducted that create parallels with reality. The uncertainties and different effects of the Internet show that the experiences that people get from it are individual, such as experiences of life offline. Traditional societies are built on direct interactions between people who live and interact with each other within the same space. However, with new technological innovations, modern societies stretch beyond the understanding of time and space. Traditions, customs and cultures were first mixed with availability to travel and migrate. However, with the spread of the Internet and social media even travelling is not necessary for cultural integration or online migration. Keeping in touch with people

[48] *Facebook,* Key Facts, Statistics 2013.
[49] Internet World Statistics 2012.
[50] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 131.

across the globe has become a matter of a click of a button. The ´barriers of time are broken by the spread of customs or traditions´ even further.[51]

Some studies on the impact of the Internet usage suggest that it reduces face-to-face communication and real and increases the time spent alone.[52] Furthermore, it is claimed to increase loneliness and depression.[53] However, here the distinction between being alone and lonely must be made. Firstly, time spent alone does not indicate its real meaning anymore, but merely means being alone in physical space. For instance, one can be alone in their private space, but still connected to the social world. The loneliness rather arises from this feature as the need for time alone, without any social encounters, is forgotten. Another reason could be if the purpose of social media cannot fulfil itself. In other words if it *´cannot compensate for the increasing difficulties of maintaining pure offline social relationships in an individualizing and busy urbanized society´*.[54]

On the other hand, the social media can influence making new social contacts and decrease the feeling of loneliness. Jan van Dijk, in his *Network Society,* claims that the individual control over making contacts is increased more than ever.[55] He brings an example of online dating that has the potential to shape the discourse of traditional means of constructing intimate relationships. The formation of intimate relationships exceeds beyond pure private matters and becomes a feature through which people experience life. As he claims, the discourse of the society changes when people no more experience love through face-to-face interactions.

*´It appears that partners with similar characteristics, attitudes and ideas are (even) more attractive in online than in offline dating. Online dating makes things easier to find someone attractive. However, it is also easy to drop out of an online relationship and immediately or simultaneously start another. In the long run this may shorten the life span of romantic and sexual relationships. After some time, the traditional skills of*

[51] J. van Dijk, The Network Society, 2nd Edition, 2006, p. 157.
[52] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 329.
[53] K. McKenna, J. Bargh, *Plan 9 from cyberspace: the implications of the internet for personality and social psychology*, Personality and Social Psychology Review, 2000, p. 58.
[54] J. van Dijk, The Network Society, 2nd Edition, 2006, p. 169.
[55] *Ibidem,* p. 235.

*courting and flirting may be lost and replaced by skills of online impression management. Communication technology can serve not only as a mediator, but also as a substitute for social contact.´*[56]

Online social media is a form of Computer Mediated Communications, which means that direct interaction is replaced by technological mediation. However, as seen above the Internet decreases the parameters of mediation and becomes the reality of social interactions. Van Dijk claims that human experience of reality has always involved all senses simultaneously. In addition to senses he brings up values, feelings and social skills. He claims that the new means of technology and social media will reduce individual learning and experience through direct action that incorporates all senses. *´As direct action remains the basis of human experience, heavy use of new media could lead to a decay of this type of learning.´*[57] For instance the importance of smell or body language when meeting a partner is diminished in online dating. Even through video conversations, the sign language comes across differently on the screen than in face-to-face communications. The interpretation of another´s emotions or intentions becomes more difficult and things are easily lost in translation. Hence, social media serves the best when individuals already are familiar with each other.[58] However, computer mediated communications allow individuals to communicate without exposing themselves to the other people and allow a greater choice of words or actions and non-verbal communication has decreased in its importance.[59] Cyberspace allows an uptake of multiple personalities and identities as one can present themselves with different age, sex, ethnicity, religion and so on.

*´This ability to carve out different identities or roles may be particularly important for those who are role poor and for those who feel that important aspects of their identity are constrained in the relationships they maintain in the non-internet world.´*[60]

[56] *Ibidem*.
[57] *Ibidem*, p. 212.
[58] *Ibidem*, p. 228.
[59] *Ibidem*, p. 235.
[60] K. McKenna, J. Bargh, *Plan 9 from cyberspace: the implications of the internet for personality and social psychology*, Personality and Social Psychology Review, 2000, p. 63.

Hence, it allows an altered reality for individuals that do not feel confident about themselves in traditional social situations. Furthermore, it is difficult to tell whether individuals are truthful about themselves online or not. For instance, one can like a song on Facebook page without actually having to listen to it. A reality can be created for the purposes of blending in or being liked. On one hand this can be positive and allow individuals to express their real nature online in the sense of being open and fearless in relation to offline relationships. On the other hand, it can be dangerous if this freedom is abused through, for example, identity theft.

Throughout human history technology has shaped the discourse of the societies. Airplanes bring us closer together; photography enables remembering of human past and the Internet access to shared knowledge. The shared knowledge and memory brings people together without having to be in the same space or time limit. When first this was available with newspapers, by creating a common human experience and understanding of reality, then with the Internet this is even further encouraged. It creates a *´chance to belong to a powerful, if imagined community, in which people feel connected to each other not because they are geographically close, but because they have socially constructed and imagined community of belonging.´*[61]

However the effects of technology cannot be measured empirically and do not have the same effect on every individual. The impact of technology on the society depends on the context of the individuals in the society. It is marked by the individual experiences and how these allow the adaptation to the changes.[62] For instance when talking about the ´digital divide´. Manuel Castells defines digital divide as inequality of access to the Internet.[63] The two categories of inequalities are positional or personal inequalities. Positional inequalities rise due to external factors that are always out of one´s control. These are defines as a particular job or occupation, education, wealth, country or region and role in a household (parent versus child; husband versus wife). The personal inequalities are age, sex, ethnicity, intelligence, personality and health or disability.[64]

[61] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 43.
[62] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 330.
[63] M. Castells, *The Internet Galaxy*, 2001, p. 248.
[64] J. van Dijk, The Network Society, 2nd Edition, 2006, p. 178.

The reference to these individual characteristics as inequality implies a situation where the incapacity to access the Internet is not an individual choice. However, the effects of the Internet on individuals depend on personal experiences of reality and cannot always be categorised as an inequality. It can also be characterised as a uniformed choice or a conscious resistance to adapt to these new technologies. For example, the digital divide in Europe due to age difference. Only 49% of individuals aged between 55 to 64 and 28% of 65 to 74 are frequent users of the Internet. Compared to individuals aged 16-24 where the Internet usage amongst high and medium formal education is 98% and 93% respectively.[65] The gap of usage between elderly and youngsters is nearly half. The research on the reason behind this mainly focuses on the lack of skills that the Internet users must possess. Certain knowledge and skill is required for searching, navigating, sorting, filtering and utilizing information online.[66] However, other reasons that affect elderly are psychological and physiological problems. They have not grown up with technology and it may seem as a foreign playfield. The elderly have a heightened risk to technophobia, which is increased by the view that everything can be done in traditional ways.[67] It can be claimed that the resistance is related to the lack of skills but moreover it is the result of mistrust in new technologies and fear of change. Firstly, young people are more likely to be capable of maintaining and extending their social networks online as the online openness of internet generation does not depend on having to adapt to the new technologies. As online world shapes the understanding of space and time, the generation, which is not born into these new concepts, will have difficulties understanding them in principal. The second and more important feature is the mistrust towards the Internet and its lack of privacy. Social media increases public openness, but this openness can have its own consequences, such as increased public scrutiny. Convincing someone to trust the new social space is not the matter of legal framework. It is rather the matter of tolerance in more open societies, which can be a difficult task to achieve and has not yet reached its potential.

[65] European Commission, Digital Agenda Scoreboard 2012, p. 8.
[66] M. Ramón-Jerónimo, *Elderly persons and internet use,* Social Science Computer Review, 7 February 2013, p. 391.
[67] K. Randver, Infoühiskonna digitaalne lõhe: selle põhjused ja mõju sotsiaalsele kaasatusele vanemas eas, 2005, p. 25.

## 2.4. Economic reality.

The progress of humanity has been influenced by new technologies throughout history – printing press, electricity, flight and so on. With each technological development the global economy has always been influenced in terms of labour, production and distribution. With digitalisation and internet the impacts are no less important. Gordon Moore argued in 1965, long before the rise of cyberspace, about the rapid development of new technologies. The phenomenon, which now is referred to as Moore´s Law, is that the computing power doubles in every 18 months.[68] Taking into account these rapid developments and the impact that they have on global capitalist systems, new economic realities are created. McKinsey study on the impact of the Internet on economy reveals several factors. Firstly their macroeconomic and statistical studies show that in developed countries the growth of gross domestic product (GDP) over the past 15 years is increased by the Internet by 10 per cent. This makes it around $500 extra in GDP per capita. Furthermore, it has increased to 21 per cent over last five years.[69] Hence, the magnitude of the benefits of the Internet to the economy is growing every year and it is further encouraged by Moore´s law. After the Industrial Revolution it took 50 years to achieve the same results as with the spread of the Internet over the past 15 years.[70] The speed of the distribution of benefits can be attributed to the adaptation and increased use of the new technologies.

The impacts of internet and digitalization on labour affect the traditional models of economy and wealth distribution. Current research in the area can be divided into two contradictory views and the future predictions create uncertainty. Firstly, McKinsey´s global survey on small and medium-sized enterprises considers the threat of internet to a job market as a myth. According to the study, even though internet has destroyed 500,000 jobs over the past 15 years, it has created 1,2 million other positions. Hence, it has created 2,4 jobs for every job destroyed.[71] William Brian Arthur does not agree with the position that internet does not threaten the job market. His claims are applicable as

[68] G. E. Moore, *Cramming more components onto integrated circuits,* Electronics, 1965.
[69] J. Bughin and J. Manyika, *The Macroeconomic Impact of the Internet,* Internet Matters: Essays in Digital Transformation, 2012, p. 4.
[70] *Ibidem.*
[71] *Ibidem.*

the study does not demonstrate the impact in developing countries that may not reach the threshold for skills and access that is required in jobs related to internet. Arthur claim that despite of the rapid growth and prosperity that internet creates, it does not create a sufficient job market and the wealth is inaccessible to many. The main challenge of the new economy has shifted from production to distribution of wealth.[72] *´For centuries, wealth has traditionally been apportioned in the West through jobs, and jobs have always been forthcoming. When farm jobs disappeared, we still had manufacturing jobs, and when these disappeared we migrated to service jobs.´*[73] However, with the digitalisation fewer alternatives can be created when the production is controlled and managed by computerised technologies. Hence, the problem is that when the wealth is created, who deserves to benefit from it if the traditional model of remuneration for work is no longer the means for distribution? How the current economic systems will adopt to the playground is unpredictable, but one thing is sure – it must bring changes to its traditional ways as the old means will not be sustainable. *´Perhaps some new part of the economy will come forward and generate a whole new set of jobs. Perhaps we will have short workweeks and long vacations so there will be more jobs to go around. Perhaps we will have to subsidize job creation. Perhaps the very idea of a job and of being productive will change over the next two or three decades.´*[74] The latter point of the changing perspectives of productivity and material values is already evident in cyberspace. The functioning of Wikis illustrates the progress of the society towards new concepts of economy that cannot be ignored in democratic societies.

With the internet era, where the production, distribution and exchange of information are eased, the flow of it has become more important than the flow of physical products. Communication and information exchange constitute the main economic activity.[75] Wikis are websites which allow people collectively share information and knowledge. People can modify, add and delete content collaboratively without having to be present in the same space and time. Cooperation between individuals can take place across the

[72] W. B. Arthur, *The second economy*, Internet Matters: Essays in Digital Transformation, 2012, p. 210.
[73] *Ibidem.*
[74] *Ibidem.*
[75] J. van Dijk, The Network Society, 2nd Edition, 2006, p. 70.

globe. The best example of the functioning of Wikis can be Wikipedia. Wikipedia is an open source of information, which means that anyone can access it without having to pay money. Furthermore, the same people who are mere users of the knowledge can also edit it. Hence, the outcome is a knowledge that is combined of different information from various sources and individuals creating ´collective intelligence´[76] Christian Fuchs writes that the motivation behind such a model of sharing information is social rather than economic. It is a good example of how the traditional values of accumulation of profit and competition is replaced by cooperation and social benefits and even though it is threatened by bureaucracy, corporate monopoly and power relations, the people keep producing it for the purpose of its free access.[77] Digitalisation and internet allow cheaper reproduction and distribution of knowledge and information, which is especially significant when considering the future of intellectual property rights. However, despite the fact that the global shift towards such models of economy still remain assumptions, the changes in economic reality have already taken place in some form or another due to internet. *´One of the more fundamental things that's going to happen is that it completely crushes the business models of a large number of organizations. A typical example is that many of the media companies are organized around content and distribution. Well, the distribution part just goes away, because distribution becomes bundled and/or free, as part of that.´*[78]

Finally, the *internet of things* has changed the ways of how companies apply market research to reach out to customers and develop new products. Internet of things is evident when information about physical objects can be communicated without human interventions due to data gathering, flow and processing.[79] It can be beneficial for companies in marketing. For instance, traditional marketing allows specific advertising of products to certain type of consumers, such as students with an assumption that they have certain interests and are unemployed. Internet, allows more personalised marketing

[76] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 135.
[77] *Ibidem*, p. 133.
[78] E. Schmidt, *Eric Schmidt on business culture, technology and social issues,* Essays in Digital Transformation, 2012, p. 202.
[79] J. Bughin and J. Manyika, *The Macroeconomic Impact of the Internet,* Internet Matters: Essays in Digital Transformation, 2012, p. 31.

because of collection of data on individual behaviour online. Amazon is only one of the websites that has personalised advertisements on an assumption based on your previous purchases. According to McKinsey, online marketing constitutes 15 per cent of total marketing spending and it is almost effortless to present goods to markets around the globe.[80] Comparing to traditional means of market research, such as surveys where people knowingly and voluntarily share their market behaviour, online marketing is automated. It can have highly economic but also social benefits such as in collection of medical data for detecting the most appropriate treatment. However, it can also have negative connotations, especially in the collection of medical data, which can be sensitive in terms of privacy.

2.5. Public reality.

Public reality incorporates the impacts that internet has on the relationship between citizens and the state. It includes features such as receiving information, increased civil societies and citizen participation that encourage democratic process. Traditional journalism is hierarchical, elite-centred and thriven by market forces and profit.[81] Internet creates a flow of information that is not subject to mainstream mass media based on what people want to hear and are willing to pay for. Often people are willing to pay more for ´yellow´ journalism that creates scandals and is follows around public figures. As general mass media is also media thriven and a closest one can get to objectivity is to collect information from various sources, internet is a tool that enables individuals to access variety of information. Furthermore, the cost of this is usually only the cost of accessing internet. *´A centralized control of public opinion by totalitarian regimes or market forces (as in the case of private media monopolies) can be undermined by internet platforms that pose opportunities for alternative information and communication.´*[82] However, such a shift is yet to take place as the monopolised media creates online access to mainstream information and the mass still trusts and pays interest into media that creates moral panics. For instance, public opinion in Estonia

[80] J. Bughin and J. Manyika, *The Macroeconomic Impact of the Internet,* Internet Matters: Essays in Digital Transformation, 2012, p. 4.
[81] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 133.
[82] *Ibidem*, p. 135.

towards the European Court of Human Rights has been shaped by the lack of education and interest. Delfi publishes up to 330 reports daily, and is the largest (free) news portals on the internet in Estonia, Latvia and Lithuania. It also allows adding anonymous comments and receives around 10,000 comments daily.[83] When the Court decided the case of *Korobov and Others v Estonia*, Delfi published a public report on the judgement. It published an article with the title *´European Court of Human Rights: Estonia must compensate to those arrested during the Bronze Night´.*[84] The article itself merely states that the State must pay almost 50 000 Euros to the violent protestors for claimed mistreatment during their detention.[85] However, it did not include any substantial information on the judgement of the court, such as the behaviour of police and the presence of medical evidence in the Court. [86] In addition, the second part of the article is titled as *´none of the claimants complained over the fairness of the arrest*,´ creating a public opinion that all the claimants took part of the criminal acts, such as vandalism. As the Bronze Night theme is still sensitive to majority of Estonian public and no substantive information was conveyed in the news, people posted aggravated comments towards the European Court of Human Rights. Even though the full details of the case and the case report are available online, people are not interested in objective analysis but rather make irrational and emotional judgements. This encourages the mistrust towards European institutions and is seen in the attitudes of public commentators: *´there is no point of paying attention to this pointless institution; let the dogs bark´; ´That is where the taxpayers money goes. People who are the perpetrators and vandals get paid for their violence. Unbelievable.´* It encourages racism towards national minorities: *´some homeless Russian person now gets paid for coming to vandalise our country.´ ´These people have not compensated a single cent. Give me the names of these bastards and I myself will end their earthly miseries. The Court of Human Rights of course does not care about the crimes of Communism´.* Finally the

[83] *Delfi As v. Estonia*, no. 64569/09, 11 February 2011 (pending).
[84] Bronze Night is reference to an uprising that took place in Tallinn durinf 26-28 April 2007. The protest started because of the city´s plan to remove a Bronze Soldier (memorial for the soldiers that had died in the Soviet Red Army during Second World War).
[85] *L. Laugen, Inimõiguste kohus: Eesti riik peab pronksiööl kinni peetutele hüvitist maksma,* Delfi.ee, 28 March 2013
[86] *Korobov and Others v. Estonia*, no. 10195/08, 28 March 2013.

lack of public education becomes evident when people in their comments claim that ´ *this decision requires the intervention of the public and stepping out of the European Union.´*[87] In an interview with the general manager and president of the largest telecommunications company in Estonia, Elion Plc, the question of why the general public does not yet pay substantial interest in information when it is so easily accessible via internet. He replied that in Western societies the main goals of the mass are wealth, power and fame. These interest are merely superficial and do not have any substantial benefits. As long as this is the case people will continue reading news that is as superficial as their pursuits in life.[88] However, over the time internet will change these goals as it changes the social and economic reality, where people will come to realisation that internet liberates in terms of public prejudice and that current models of economy (including the monopolised media) are not sustainable. Furthermore, the diversity of education becomes available for the purpose of increased objectivity. All citizens can become journalists and conveyors of knowledge. Currently, this does not mean that people are listened as information sharing *´today takes place in a hierarchical and stratified society in which public attention can be bought and is controlled by media corporations and political elites.´*[89] Taking full advantage of the benefits of internet is still at a primary stage but this will change as other opportunities are being realised. The people who are in power, be it companies or politicians have to follow the will of masses, that becomes accelerated and open in internet, at some point. *´It is the single best argument for democratic expression, but more importantly, personal individual freedom that has ever been built.´*[90]

Another great development that becomes available thanks to internet is the e-democracy and e-state. Because of internet the State can provide services, to citizens at much lower cost. Such services include tax, social and health services.[91] Additionally, internet

[87] L. Laugen, *Inimõiguste kohus: Eesti riik peab pronksiööl kinni peetutele hüvitist maksma,*Comments 1-20, Delfi.ee, 28 March 2013.
[88] Interview (in Estonian) with Arti Ots, General Maganger and President of Elion Plc, Tallinn, 12 April 2013.
[89] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 135.
[90] E. Schmidt, Personal Democracy Forum, 2007, min.14:05.
[91] J. Bughin and J. Manyika, *The macroeconomic impact of the Internet,* Internet Matters: Essays in Digital Transformation, 2012, p. 8.

encourages political participation for citizens in form of electronic voting and electronic forms of consensus. Digital memory that is achieved through connecting individuals online and collecting their data improves *´the precision of government decision-making on the individual as well as the societal level. When individuals apply for government service, comprehensive digital memory may lead government agencies to render more accurate decisions*.[92] Hence, e-government is the core to integration of economic, social and environmental planning as well as citizen participation in the activities of the state. The major obstacle of effective development of an e-state is the trust of the citizens in online services. For instance, in terms of data collection for the purposes of improving public healthcare services. The active participants of an e-democracy must be certain of the consequences that happen as a result of their actions online – that their actions will not have consequences similar to the case of Stacy Snyder. Secondly, the freedom of internet and the flow of information must allow criticism of the government without threat of being scrutinised without valid reason. The reasons are only justified when collectively accepted by the society and without imposition of power. The internet does not only potentially encourage the development of democracies, but also the transition to democracy. During the rise of Arab spring social media helped to spread the revolutionary across the region because it allowed the spread of messages *´about democracy, liberty, and freedom, as opposed to economic issues or Islam.´*[93] This is a direct result of a space where anyone can access anything. Amongst the first things that oppressive regimes would do is trying to create a confined space that follows specific rules. With internet, however, even in the case of blocking access to certain information, technologies can cross any barriers or ´borders´ of internet (for instance, with proxies). Furthermore, as the internet does not limit itself to a specific time and space, the restrictions to use it are only real when disabling access to cyberspace completely. The public space that is created by internet flows across borders of nation states. The unity of people and one public space is no more dependent on similar characteristics of individuals. *´What binds people in a contemporary public sphere is not a fixed number of common situations, views, habits and other social, cultural and political*

[92] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 94.
[93] S. Joseph, *Social media, political change and human rights,* Boston College International and Comparative Law Review, 2012, p. 166.

*characteristics. It is an extremely diversified and shifting complex of overlapping similarities and differences, particularly in the growing number of multicultural societies.´*[94] However, the claim of differentiating between the impacts of internet on more or less multicultural societies does not remain valid anymore. Internet creates one global public sphere where multicultural state, as such, seizes from existing. No borders create a reality where the whole cyberspace is multicultural, regardless of the physical location of the individual.

## 2.6. Conclusion.

With the creation of World Wide Web marked the beginning of internet revolution. It increased user-friendliness making the networked information accessible to general public. When such a powerful tool for creation, access and exchange of knowledge reaches to the people, then the progress of the societies takes a new discourse. Internet serves equally important purposes in the social, economic and public spheres of people´s lives. It becomes so essential for functioning of modern societies that it becomes a new reality and space for life to happen. With the rise of social media internet allows individuals to communicate with no limits of space or time. Individuals can easily share information between each other and enforce their right to maintain and establish relationships at ease. Social space becomes reality due to variety of experience that people subtract from the social media. It creates a new space for integration as people can exist in the same space while physically being apart. The effect of internet varies depending on individual circumstances. It can create emotions of loneliness or courage, depending on past and present experiences. It is unlikely that people experience cyberspace the same way, as it is unlikely that everyone has the same life experience. For instance, elderly have more difficulties in adapting to internet communication because they have to change their old ways. The internet generation, however, do not have to adapt as they are already born into the network society. In addition, social space allows presenting oneself with a completely different identity than in offline space. Internet allows individuals to globally reach businesses and vice versa. Whether the impact of it to job market is positive or negative can be debated. However,

[94] J. van Dijk, The Network Society, 2nd Edition, 2006, p. 173.

it is clear that it impacts it in ways that directly affect people´s welfare. The economic impact that affects the way people experience life. Cyberspace influences the shift of traditional models of business and free market. Sharing of information and knowledge becomes the main economic activity and allows the creation of shared memories and collective intelligence. The new models of sharing knowledge affect the relationship between citizens and the state. Traditional profit orientated journalism is overthrown by public who take a new role of being public watchdogs. Cyberspace has the potential to encourage democracies as it increases public participation in the matters of the state. Because the gravity of impact of cyberspace on everyday life is so great, it creates a completely new space and virtual reality. New reality causes the shift of reasonable expectation of privacy and old rules cannot be applied to new space.

## CHAPTER 3

Reasonable expectations of privacy in cyberspace.

### 3.1. Introduction.

Private reality on internet, as with any other parameters of privacy even offline, requires some form of public or social reaction to really become private. Unless the relativity between privacy and public sphere is upheld, no individual would consciously admit to oneself, than the preformed action is private. Hence, privacy is always relative to public interactions. Cyberspace can serve for social, public and private purposes at the same time (even literally) and therefore, it cannot be confined to one single form of ´space´. Hence, every action individuals perform online can be misinterpreted or abused for an unintended purpose. In cyberspace every action can become private because the risk of being susceptible to public interactions. Traditional understanding of privacy and public has shifted because the cyberspace itself has intervened with private matters of its users. For example, how traditionally the right to maintain and establish relationships has been exercised.

Because the clear distinction between private and public diminishes in cyberspace, it must be distinguished from traditional theoretical considerations by the Court. Furthermore, because their private actions can be easily scrutinised by public

interactions, individuals have to continuously think through how they use internet. This can have very positive implications if people can remain also their private space in online world. If this requirement is not upheld, it may encourage mistrust towards internet and have a chilling effect, which becomes a barrier to a progress of democratic societies. However, it is as difficult to regulate freedoms on internet, as it is to distinguish what is private and public in cyberspace. This is where all human rights problems that might rise online begin – the difficulty to balance the rights and responsibilities on internet.

### 3.2. Privacy concerns in cyberspace.

When individuals open up in social or public sphere which does not have limits in space and time, they also subject themselves to increased moral judgements. The case of Stacy Snyder, even though, outside of the European jurisdiction, is a perfect example to illustrate how the social norms have not been adopted to the new reality. Stacy Snyder was applying for a job as a teacher in Millersville University and had achieved all necessary qualifications for the position. However, she was refused with a justification that her behaviour was not appropriate for the future teacher. This was because she had a picture of herself on a social networking site MySpace that had a caption of ´drunken pirate´. The photo merely showed her wearing a pirate hat and drinking from a plastic cup. Her case was dismissed in the court because the attributes of privacy in such a case were not protected by the First Amendment.[95] One problem here is that the legal protection of privacy has failed to progress with the new technology, but the bigger concern here is the prejudice that has followed a photo that has been intended to be shared only with selected people. Prejudice is defined as an unfavourable opinion formed without thought, knowledge or reason. In this case Stacy clearly has become a victim of mere prejudice as it was impossible to identify that she is drinking alcohol. Even if she was, she is old enough to do that and this factor should not have any impact on being a teacher in University. Furthermore, sharing files, pictures, videos and private information online has become widespread because it is the key to keep memories alive

[95] *Snyder v. Millersville Univ.*, No. 07-1660, 2008 U.S. Dist. LEXIS 97943.

and create a common experience with families and friends.[96] It can be assumed that if similar case would reach European Court then the big part of the assessment would include the principles of public privacy. That she only intended this picture to be seen by certain number of people and the access to third parties is a failure to provide appropriate protection of private data. However, in its attempts to protect privacy on internet through such means, it does not rule on matters of social prejudice as a result of interference of privacy. If Stacy posted a picture that titles, for example, ´dedicated socialist´ then her refusal for employment would qualify as discrimination. Article 14 of The European Convention on Human Rights reads that:

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.[97]

Hence, her privacy must be protected without prejudice to any of the characteristics named above. All these features that are protected under article 14 qualify as matters of privacy themselves. However, the question arises whether the internet and social networking have created new dimensions of privacy that should not be discriminated against as they portray the right to form relationships, identity and personal autonomy. As young people grow older and adults adapt to the culture of online world of photos, diaries, commentaries and friendships the digital divide between the youth and the elderly disappears naturally and the whole society becomes connected through online networks. However, Viktor Mayer-Schönberger claims that because of this, the case of Stacy Snyder will become paradigmatic for the whole society, rather than to one generation.[98] The result of this progress can be opposite – if such behaviour becomes the norm it will disrupt the coexistence of human beings in the society and the social norms will change. In his interview with Thomas Friedman, Eric Schmidt, the chief executive officer of Google, said that *´people are going to be much more careful about how they talk to people, how they interact with people, and in particular, what they*

[96] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 27.
[97] Art. 14 of the European Convention on Human Rights.
[98] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 3.

*offer of themselves.´*[99] This is the implication of the current society that is based upon prejudice towards purely private matters. With the increased knowledge of people and the progress of the society such prejudices will eliminate themselves as they have done with other features of privacy, such as homosexuality or inter-racial marriage. Now the task of the Courts in Europe is to encourage elimination of prejudice, based on private features, in matters that are out of individuals control and occur between social and public space.

Internet and cyberspace create variety of human rights concerns. This is either because it is an open space with no borders or limits of time. There is so much information available to people. This perception towards this information can vary from people to people and countries to countries. Some form of expression online is seen as harming others. Due to the diversity of individuals, and the unlimited opportunities in cyberspace, the information in internet becomes uncontrollable. Due to this, the main analysed human rights problem of cyberspace is the freedom of expression.[100] Freedom of expression, as any other freedoms, requires some responsibilities towards the society. Article 10(2) of the European Convention on Human Rights acknowledges this. *´The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society.´* There is a threat that if the speech gets out of hand, then it potentially creates other violations of human rights, such as discrimination or incitement to violence. However, what differs in online is that protecting the rights of others becomes very difficult, if the immoral act is conducted in a perceived private space. In traditional societies there has been the assumption by the people that if one is not caught on action, one is not guilty of an immoral act. This raises another concern online - surveillance. The concern of the surveillance online is that it is difficult to distinguish the line between intrusion of privacy and justified reason. Surveillance becomes subtle but overarching, because of the amount of data that can be collected and stored relatively quickly and cheaply, which threatens the right to privacy

[99] E. Schmidt, Personal Democracy Forum, 2007, min. 23:16.
[100] Aricle 10, European Convention on Human Rights.

of everyone in cyberspace. All human rights concerns that are generated by internet can be, to an extent, linked to privacy.

Internet as a tool for spreading and accessing information creates another theoretical concern. Acquiring information about our surroundings, helps us survive. Hence the power of knowledge as a concept is rooted in human behaviour historically.[101] Access to internet is a tool to empower individuals in the modern democracies. People, who do not have access to the communication networks or the skills to put it to use, become powerless.[102] *´What is happening now is that if you are not online and you don't have access to the kind of information that all of us in the room have, you don't really have access to modern world. Powerful notion of having a computer that is so personal it understands almost the way you think or at least can mimic some of the things the way you think.´*[103] The first point implies the technological dependence of individuals to be empowered in the society or to have access to the modern world. On the other hand, technology is developing so radically that computers can understand how people think, which itself can be considered interference with privacy. Hence, the problem of adjusting privacy to private reality online is not only the question of legislation, but also a question of the extent that society is willing to adjust its own understanding of ´private´.

### 3.3. Adopting the right to privacy, as established by the European Court of Human Rights, to virtual reality.

In order to conclude how cyberspace changes the traditional understanding of private reality, the opinions of the Court and theories of privacy offline must be applied to special characteristics of internet. First, as the case of *P.G and J.H* established, private life considerations arise when systematic or permanent records, of the material obtained in public domain, comes into existence. This potentially creates a situation whereby all forms of data gathering and storing threatens privacy, especially, if cyberspace is perceived as a public space. In this case, as the creation of data took place in private

[101] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 97.
[102] J. van Dijk, The Network Society, 2nd Edition, 2006, p. 95.
[103] E. Schmidt, Personal Democracy Forum, 2007, min. 02:29.

rather than public domain and did not include gathering in terms of the content, no interference with privacy took place. However, in cyberspace the public or private domain cannot be distinguished. The court in *P.G and J.H.* said that ´ *It is not in dispute that the obtaining by the police of information relating to the numbers called on the telephone in B.'s flat interfered with the private lives or correspondence (in the sense of telephone communications) of the applicants who made use of the telephone in the flat or were telephoned from the flat.*´[104] If a similar view is applied to the cases of cyberspace, then the first part of the test applied by the court will always be fulfilled. Individuals are most likely to access internet while being physically in a private space. Hence, this approach cannot by applied online as it is offline. Similarly, the generalisation of internet as a public domain undermines the private reality created by cyberspace. For instance, the Court has acknowledged that features such as gender, name, sexual orientation and religion are all subject to the right of privacy. Internet allows conscious altering of these features that are private, as people can change their virtual identities. Hence, in virtual reality, people have high degree of choice and autonomy in terms of private features, which traditionally are not a choice. The right to privacy requires consideration whether ´private´ is the virtual identity itself or attaching it to the physical individual in offline space. Furthermore, in *Peck,* failure to mask the identity amounted to disproportionate interference and disclosing data to third parties must be consensual. This route can be applied to protect some problems of privacy that occur online. It becomes much more difficult to have an overview or control the access and leakage of data, in cyberspace. Hence, if the individuals cannot sufficiently exercise control over their information online, then they also cannot consent to its movement. Privacy in public spaces arises because individual has a choice of the extent of the private information it reveals to public around. He or she also has a choice of the public that he or she exposes him- or herself to. It can be difficult to differentiate between public or private space online. In addition, what becomes public space online does not leave any immediate overview of the others who are the ´public´ and, hence, becomes infinite. This divides the public place and social space. Online social space is defined by social actions (blogs, sharing files, social networks etc.) and requires some ethics of

[104] *P.G. and J.H.* v. the *United Kingdom*, no. 44787/98, ECHR 2001-IX, §42.

behaviour that is characteristic for ´public space´. However, online social space allows greater amount of choice than online public space. In the social space, the individuals can choose the extent of the audience of their actions. Because of this reasonable expectation of privacy, higher degree of protection is required according to perception of privacy by the users. Top-down approach to privacy concerns is no longer sufficient in online environment.

### 3.4. Surveillance in cyberspace.

Surveillance refers to any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered.[105] Interference with privacy has been defined as interference with physical and psychological integrity. The first requirement for the interference to be allowed is that it must be in accordance with the law. In order to preserve democracy, the Court has also established that the laws must follow the rule of law, hence, be accessible and foreseeable so that individuals are able to regulate their conduct. Surveillance becomes a method of enforcing criminal law because it makes individuals regulate their conduct. However, it can be argued that legitimacy of surveillance requires a high degree of transparency and rule of law. According to the Court, surveillance is only tolerable if it is safeguarding democratic institutions.

Both private corporations and government agencies take advantage of the increasing technical capability of information systems to collect and process consumer and citizen data. They use this vast amount of data to build profiles to acquire knowledge about consumer preferences for commercial purposes and citizen behaviour to detect and prevent security breaches, fraud, terrorism and other crimes.[106]

The emergence of the internet has created a new platform by which surveillance can be carried out which in turn requires a new regulatory framework. Although similar methods of surveillance were used by government and corporations before the advent of the internet, its emergence allows individuals to be surveyed on a more intimate and

[105] T. Dinev, P. Hart, M. R. Mullen, *Internet privacy concerns and beliefs about government surveillance – an empirical investigation*, Journal of Strategic Informations Systems, 2008, p. 215.
[106] *Ibidem.*

deeper level. An everyday life example would be of a husband that spies on his wife. He uses a computer program to find out her passwords, reads her e-mail because he doesn´t trust her, and finally threatens her because he finds out private information that she wanted kept secret. This is form of surveillance is made possible by cheaper means of storing data.[107]

Certain forms of electronic surveillance could be acceptable if citizens were aware that they were being monitored and thus self-disciplined themselves to behave in a certain, more positive, way. Indeed, surveillance is a tool for crime prevention. In Britain millions of CCTV cameras have been installed to prevent crime. Although studies have shown that crime rates dipped only marginally, it was discovered that the police did not have enough staff to properly browse through the recordings.[108] Nevertheless, when surveillance is carried out in secret, without proper oversight and public scrutiny, it has the effect of infringing upon individual autonomy. Individuals are denied the right to consciously take decisions on how to behave correctly, and through that shape the social discourse. French Philosopher Michel Foucault, who addressed the nature of power and how it is used as a form of social control, applied Jeremy Bentham's panopticon design as a tool to help understand the effects of surveillance on individual and societal behaviour.[109] Although Foucault's work has been widely influential, some would argue that it is not suitable for analysing surveillance in an information society, as surveillance would no longer serve a single coherent purpose of control and would now also be conducted by private actors.[110]

However, electronic surveillance by corporations and nation states do aim at controlling the behaviour of individuals and groups. Corporations conduct market research in order to predict the behaviour of consumers. The power to predict also gives the power to shape consumer behaviour. Individuals are threatened by the violence of the market, which wants to force them to buy or produce certain commodities and helps reproducing capitalist relations by gathering and using information on their economic

[107] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 271.
[108] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 103.
[109] C. Fuchs, Internet and Society: Social Theory in the Information Age, 2008, p. 268.
[110] *Ibidem*, p. 267.

behaviour with the help of electronic systems.[111] In the case of states, individuals are forced to behave or not behave in certain ways because they know that their appearance, movements, location, or ideas are or could be watched in electronic systems. Information leaked by government whistle-blower Edward Snowden, an infrastructure analyst for the NSA and ex-CIA employee, was ranked as the most significant breaches in the history of the NSA.[112] It showed that the NSA focused on getting information from any source through whatever means to best serve the interests of national security. The NSA targets the information of everyone by default considering it to be the most efficient way to combat terrorism; even if you are not doing anything wrong, you are being watched and recorded. It has gotten to the point where you simply have to fall under suspicion of somebody, even under wrong call. Then the system can be used to go back in time to scrutinize any decisions of the past. This allows painting anyone in the context of a wrongdoer. It is this element of control in behaviour and ambiguity of existence that makes surveillance so dangerous. It operates with threats and fear, and it is a form of psychological and structural violence that can turn into physical violence.[113] Foucault even stated that, ´surveillance is a power that is capable of making all visible, as long as it can itself remain invisible´.[114]

If the public are to be surveyed, they are owed an explanation of the intentions. Hence, it must be conducted in transparency. Subverting the power of government, to corporations, is fundamentally a threat to democratic society. The public needs to decide whether these policies are right or wrong. Data surveillance requires greater scrutiny and a balance must be found between protecting people's privacy and giving law enforcement sufficient powers. Furthermore, due to an ideological twist, individuals are not only afraid of social insecurity but are continuously told that becoming a victim of crime is the largest threat; which can cause an increasing willingness of citizens to support surveillance and law-and-order politics.[115]´*The outcome is a culture of distrust*

[111] *Ibidem*
[112] S. Shane, R. Somaiya, *New leak indicates Britain and U.S tracked diplomats*, The New York Times, 16 June 2013 The New York Times.
[113] *Ibidem*, p. 270.
[114] *Ibidem*, p. 268.
[115] *Ibidem*, p. 275.

*and control.´*[116] However, the emergence of the ´right to forget´ in cyberspace, attempts to return the control of private information to individuals concerned.

3.5. The right to forget.

Cyberspace creates difficulties in establishing precise relationship between private and public. It undermines the traditional measuring of relativity that privacy has in terms of public interactions. First, this creates a problem where people are unaware or confused in terms of their rights, freedoms and responsibilities. However, it also creates a space where individuals put themselves into a position of judgement and public scrutiny. This becomes a problem if people are unaware of the amount of private information that available online. For instance, a report by McKinsey Global Institute suggests that 30 - 40% of citizens of all age groups in the research countries do not know what information is available about them online.[117] One reason for the unawareness is that the flow of information online can easily become out of control. On the other hand, information can only get online as a result of a positive act by the individual concerned. For instance, using search databases or purchasing something from internet store. The unawareness of the personal information arises because people themselves cannot remember details of every time they accessed internet. *´Google knows more about us than we can remember ourselves.´*[118] Eric Schmidt has expressed his concerns towards the memory of internet, which creates a danger of creating a situation where individuals can be judged upon actions of the past. *´One of the problems we are having is that we are developing a lifetime of memories, not everyone of which we want people to know. I think everyone has a set of things you did in high school and want to be forgotten. And as you get older you begin to understand that your actions are consequential that you don't understand at a certain age.´*[119] People can no longer run away from their past. Hence, when analysing or regulating internet, it is important to consider the impact of forgetting on human evolution. This right is

[116] *Ibidem*, p. 272.
[117] World Economic Forum, Norms and Values in Digital Media: Shaping Solutions for a New Era, 2013, p. 8: The countries of research are US, UK, Russia, Germany, Spain, Netherlands, France, Poland, Italy, China and Brazil.
[118] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 8.
[119] E. Schmidt, Personal Democracy Forum, 2007, min. 02:29.

Viktor Mayer-Schönberger has written a comprehensive analysis of the right to forget in the era of digitalisation. He acknowledges that the ´world brain´ created online allows humans to create a database of infinite knowledge. However, human brain deliberately erases great amount of information before it reaches long-term memory.[120] In addition, it adjusts what we remember according to our past experiences and current preferences.[121] Because the perception of individuals towards themselves and their surroundings changes over time, there is no objectivity of the criteria by which people make their judgments. *´If we all switched from individual human to external digital remembering, and thus gave up our ability to see our past through the eyes of who we are in the present, the individuals´ ability to control information would become perverted.´*[122] There is a danger that external memory and artificial recalling de-attaches people from the emotional or contextual circumstances of the memory. Hence, individuals lose control over the ´truthfulness´ of the memory. It can be argued that humans have too little control over what to remember or forget. However, remembering in human brain usually follows an emotional recalling, which is absent in digital remembering. *´Since the beginning of time, for us humans, forgetting has been the norm and remembering the exception. Because of digital technology and global networks, this balance has shifted. With widespread technology, forgetting has become the exception, and remembering the default.´*[123] Forgetting enables people to let go of their past and make rational decisions. The same happens with the societal forgetting that *´gives individuals who have failed a second chance.´*[124] Hence, forgetting allows people to forgive themselves and others. If this ability is reduced, individuals become subjected to increased public scrutiny. Furthermore, the extreme scrutiny will result in individuals losing their uniqueness. As the uniqueness itself can be subjected to prejudice, the individuals who become subjects of scrutiny, will lose their moral personalities.[125] Forgetting in cyberspace becomes a right that is vital for preservation of diverse and

[120] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 17.
[121] *Ibidem*, p. 20.
[122] *Ibidem*, p. 107.
[123] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 2.
[124] *Ibidem*, p. 13.
[125] *F. Schoeman, Privacy: philosophical dimensions of the literature,* Philosophical Dimensions of Privacy: an Anthology, 1984, p. 19.

heterogeneous societies. It also plays an important role in reducing the intolerance and prejudice, such as in the case of Stacy Snyder.

Recent proposals by the European Commissions for a regulation, on the protection of individuals with regard to the processing and free movement of personal data, expressly refer to the right to forget online: *´Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed or where data subjects have withdrawn their consent.´*[126] In cyberspace the movement of data is very difficult to control. This provision creates a right to forget as it requires erasure of personal data on request or informing of people how the data is used. However, the power for individuals to control their personal information is increased only to an extent. If taking the example of social media, it requires the service providers to erase the data completely, after the individual gives such a command. Hence, there is automatic assumption of consent that is revoked by a positive act by an individual. Furthermore, it is nearly impossible to monitor third party access to data, without intervening with the right to privacy. The second problem is that the ways how data is used is usually expressed in the terms and conditions of the accessed site. However, even if people are informed that data is collected, they remain unaware of the reality of the consequences. This piece of legislation fails to fully protect the right to forget, because it does not affect the increased prejudice of people in cyberspace. However, the General Data Protection Regulation overall is a positive step by the European Union, as it recognises and attempts to balance the benefits of digital remembering with the potential harms. For instance, by allowing data collection and processing only for certain period of time and purposes. It is significant as it illustrates that Europe is starting to realise that special characteristics of cyberspace require adapting the right to privacy in a new manner.

[126] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 25 January 2012, §53.

3.6. Responses of the European Court of Human Rights.

The Court and member states of Council of Europe recognise the problems of privacy that arise in cyberspace. Amongst these problems are the existence of the software that is capable of collecting and storing data, including personal data (e.g. keystrokes that reveal passwords). Moreover, access to and storage of private information by third parties such as user generated content, websites visited, and geographical locations that potentially allow tracking and surveillance by the government and third parties. This data can reveal delicate and sensitive personal information (such as financial, health, political, religious and sexual preferences), which can aggregated into profiling of individuals.[127] Firstly, profiling encourages prejudice and false impressions. In *Copland* for example judges stress the privacy of work email and internet usage history and view it as prima facie covered by the notions of private life and correspondence for the purposes of Article 8(1). This case raises two major issues: the storage of the data by third parties and lack of legislation to regulate such activity, in cases where it might be required for public good.

Search engines play a crucial role in achieving the benefits of cyberspace, such as access to information, opinions, facts and ideas, as well as other content, including entertainment. Such access to information is essential to building one's personal opinion and participating in social, political, cultural and economic life. As such they become an accumulator of personal information on the users. Due to their mode of operation, search engines tend to save the user data in order to improve the software and service[128]. In addition the government monitoring of the searches and social networks for keywords, which only recently became known to the public, only emphasizes the need for protection of people's privacy.

Social media has "*a great potential to promote the exercise and enjoyment of human rights and fundamental freedoms*"[129]. "Social networking services offer the possibility

[127] Council of Europe, Declaration of the Committee of Ministers on Risks to Fundamental Rights Stemming from Digital Tracking and other Surveillance Technologies, 11 June 2013.
[128] *Ibidem.*
[129] Council of Europe Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services, 4 April 2012.

both to receive and to impart information. Users can invite recipients on an individual basis, but in most cases the recipients are a dynamic group of people, sometimes even a mass of unknown people (all the members of the social network). In cases where users' profiles are indexed by search engines, there is potentially unlimited access to parts of or all information published on their profiles"[130].

One of the major recent steps is by the Council of Europe is the Declaration of the Committee of Ministers adopted on 11 June 2013, which sets a framework for states to apply their negative and positive obligations to govern and protect privacy in cyberspace. Even though it is only recognition of the problem and leaves states the margin of appreciation of applying it, it signifies the European approach to surveillance. The Committee *´alerted member States to the risks of digital tracking and other surveillance technologies for human rights, democracy and the rule of law and recalled the need to guarantee their legitimate use which benefits individual; and welcomed measures taken by both State and non-State actors to raise awareness among users, and, a fortiori, within the private sector and among technology developers about the potential impact of the use of such technologies on human rights´*[131].

Another step forward was made by Recommendation to member States on the protection of human rights with regard to social networking services adopted in April 2012. Among number of recommendations the most important ones were: to encourage search engine operators to inform the users of disclosure of any information about them to anyone to be in accordance with art 8; to create a system that enables users to have prior knowledge of possible interference of the data, as well as to have control over it; and to have to pseudonym. *´It is important for users to be able to feel confident that the information they share will be processed appropriately. They should know whether this information has a public or private character and be aware of the implications that follow from choosing to make information public. In particular, children, especially teenagers, and other categories of vulnerable people, need guidance in order to be able*

[130] *Ibidem.*
[131] Council of Europe, Declaration of the Committee of Ministers on Risks to Fundamental Rights Stemming from Digital Tracking and other Surveillance Technologies, 11 June 2013.

*to manage their profiles and understand the impact that the publication of information of a private nature could have, in order to prevent harm to themselves and others.´*[132]

3.7. Conclusion.

Privacy in cyberspace is relative to what is considered public. No individual would consciously think about privacy, unless some information has become private due to public interaction. Cyberspace cannot be defines as one space. It can be difficult to establish the reasonable expectations of privacy online in a way that is applicable to everyone. Cyberspace places individual´s information under greater public scrutiny, and people would consciously have to think about every action they perform online. However, as the Internet becomes a new reality, this would not be the most desirable way to operate it. The example of Stacy Snyder illustrates how the legal protection of privacy is out-of-dated. More importantly, it is an example of how the prejudice in the society becomes a problem in terms of online privacy. The widespread theory that knowledge is power creates a technological dependence of internet that empowers individuals. However, the power of knowledge is shifted with the creation of big data. Similar freedoms must be allowed in virtual reality as in offline world. Gathering and storing a mass of data becomes a problem if it is done in a systematic manner and takes a form of surveillance. Firstly, surveillance can be used as a form of social control by the state and by big businesses. Secondly, surveillance intervenes with individual´s privacy due to its power to shape autonomous choices and behaviour. Policies of covert surveillance create a culture of distrust and control. However, the global society of legal thinkers has talked about the new right to forget online. This aims at shifting the control over information from states and corporations back to individuals. It becomes essential because people are unaware of the extent of information that is available about them online. The right to forget has also been emphasised by the European Commission. However, the main concern of the proposed regulation is that it does not fully deal with all the privacy problems that arise in cyberspace. For instance, it does not take into account the consequences of increased prejudice, such as, in the case of Stacy Snyder. The European Court of Human Rights and Council of Europe have also recognised

[132] Council of Europe, Recommendation CM/Rec(2012)4, 4 April 2012

privacy problems only to an extent. They have pointed out problems of privacy, such as storage of data, surveillance and general threats of being visible online. However, not enough cases on online privacy have reached the Court, in order to have fully developed protection of online privacy in Europe. The problems of privacy in cyberspace reach far beyond what has been established by the current legislation in Europe. This can be seen in the case of copyright enforcement, which arises much bigger concerns regarding the chosen policies for governing European countries.

## CHAPTER 4

Privacy concerns in copyright enforcement strategies online.

### 4.1. Introduction.

Copyright can be considered protecting the right to privacy, as it serves the purpose to protect the freedom of conscience and ideas. The first part of this chapter will look at the history of copyright and the purposes it serves. Furthermore, the economic dimensions of copyright will be looked in order to assess the impact it generates on the copyright owners. The right to be part of the benefits created by artistic expression or scientific advancement has been granted by the Universal Declaration of Human Rights. However, digitalisation and the spread of internet have shifted the traditional models of communication and business. This affects also the application of copyright laws to the new reality. For instance, peer-to-peer networks, which allow instant sharing of knowledge and information between individuals. The policy reactions to peer-to-peer files haring vary from country to country. Firstly, the most common model of criminalisation of sharing copyrighted works will be assessed with an example of France. Secondly, the Canadian approach of legalising copying for private use, will be examined.

4.2. History and theory of copyright.

The first copyright laws were created during 18th century with the spread of printing press. The spread of printing press allowed easier reproduction of books than previously with having to copy them by hand. Governments teamed up with publishers to maintain the control over access to books and spread of knowledge. This information control was a great tool to maintain the power as it is built up on knowledge and education; hence, the books could only be printed after approval by the government. However, such a power relation would mean that it is not only in the hands of the government but also the publishers themselves who now could exercise direct control over the publishing of the books, rather than the state. It has been argued that the Copyright Act 1709 was created because the control of the publishers had exceeded the will of Queen of England and potentially threatened the power of the state. The purpose of Queen Anne´s legal invention was to limit the control of the publishers by empowering authors.[133] It is evident that people have understood the power of knowledge for centuries. Furthermore this power is the consequence of the control and access to it. This brings the first notion of copyright as a right to privacy itself. Ultimately privacy has been considered as the power of an individual to exercise control over information about him. Especially in modern liberal societies that are built on the principles of personal autonomy, the right to privacy become the right to make conscious choices over whom, when and how access one's personal information regarding identity. Hence, copyright is a right to privacy itself as starting point for intellectual property is creativity and private thoughts that later are made public. *´The laws of copyright have been created to protect privacy interests. The protected interest is the extent of which individual´s thoughts, emotions, feelings become available for others, which clearly is a matter for privacy laws.´*[134] Hence, the protection of copyright can be seen as a protection of privacy in public places similarly to the public privacy principles established by the European Court of Human Rights, which create reasonable expectation regarding access and distribution of

[133] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 98.
[134] *F. Schoeman, Privacy: philosophical dimensions of the literature,* Philosophical Dimensions of Privacy: an Anthology, 1984, p. 15.

personal information. In addition, following this approach copyright and the right to privacy therefore become indistinguishable.

Richard Posner argues that the personal privacy rights are not distinctive from other rights and can be creating harm in itself because it is deceptive and not economically efficient. He believes that the right to privacy should be systemized in a way that maximizes investment into producing and communicating socially useful information. The right to privacy should only be granted in cases where otherwise it would have a negative effect on the freedom of communications.[135] However, his approach is extremely pretentious as it takes a superior position itself and allows the superiority of someone to decide on what is socially useful information without taking into consideration that intimate relationships and other communications, that under his view are not socially useful, actually shape the social discourse and encourage progress. This superior position allows the labelling of individuals that do not match the criteria, for deserving privacy, as inferior and leaves them without a right due to subjective assessment of one´s consciousness being more significant than another´s. Here the distribution of the right to privacy becomes discriminatory and it gives a rise to privacy as a distinctive right with no exhaustive definition. Furthermore, it excludes the individuals, who do not prioritize economic interests over other values, from the right to privacy. Therefore, this materialistic view diminishes the individual autonomy as it does not allow the freedom of consciousness in terms of prioritizing different values in life.

The second reference to copyright as a human right arises from the Universal Declaration of Human Rights 1948. Article 27 states that:

1. Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.
2. Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

[135] *Ibidem*, p. 29.

In other words, on one hand, everyone has the right to be part of the benefits that is created by artistic expression or scientific advancement. As the Declaration was drafted right after the Second World War, the first paragraph has its own historical connotations. The initial purpose of it was to prevent the abuse of science and technology for atrocious reasons.[136] Even though, this did not realize until mid-1990s as the Cold War significantly slowed down scientific process in areas other than warfare, the footmark was created for equal opportunity to be innovative. Furthermore, it created a doorstep for open artistic creation as it intended to prevent abuse of creativity for the purposes of propaganda only.[137] The second paragraph, on the other hand, creates a right to moral and material interest of the scientists or artistic creators. Hence, it creates an explicit right for intellectual property. It must be noted that as it protects both, moral and economic interests, it does not take a stand on which theoretical position should apply to the protection of copyright. Whether it is the moral right to one´s private thoughts or economic interests, both approaches must be protected. The right to material interest gives way to the legal approach of protecting copyright as a right to property.

The legal recognition of property right originally protects the physical possession of goods. The creation of intellectual property rights is a legal fiction but serves a similar purpose as behind every property there is an owner and with copyright the owner is the creator of the work or whoever purchases the right. As intellectual property, the property of an idea, does not exist in a tangible form, it cannot be in a physical possession. However, the protection of it is as valuable to the society because of the benefits that it gives in the form of cultural heritage and the fact that the production of all material goods begins in the mind of the scientists or creators.[138] Hence, this allows the rise of the view that copyright should be protected in the similar ways as physical property and violation of the right by individuals can be considered as a theft. In addition, it can be claimed that, in theory, the protection of intellectual property is even more important to liberal democratic societies than of tangible objects in possession. The principles of liberalism are built on belief that all individuals have a right to believe

[136] P. Torremans, Copyright and Human Rights: Freedom of Expression, Intellectual Property, Privacy, 2004, p. 5.
[137] *Ibidem.*
[138] *Ibidem,* pp. 3-4.

that what they believe is right. In addition, it is founded on individual autonomy based on personal interests that people have when they make decisions to act. Hence, intellectual property must be protected in order to encourage creativity and scientific advancement in the society. However, in liberal societies the encouragement of creativity is only attributed to material (or any other) gain. Only because individuals have selfish goals they are willing to be innovative, which then, progress the democratic societies. When the laws protect copyright, they do that in order to encourage creativity, which in itself is a valuable interest of the society. The principles for protection in democratic societies are based only one strain of thought, which are liberalism and free market.

4.3. Impact of digitalisation on copyright.

Digitalisation; revolution of information and communication technologies; and internet, have the power to change the conventional theories of copyright protection. Firstly the power that is created by the control of information takes a radical shift. Exercising control over something measurable in certain territory, space and time is no longer possible online. Everyone can be creator and receiver of information and ideas. If in the past, the artists who create music or film had to look for help from corporations to spread their work and get recognition, then with internet this feature is less of importance. Artist can upload their creations on internet and share their works in a much easier manner and do not have to turn to companies that become owners of their copyright. The concerns that the current functioning of music industry does not encourage creativity, but mere profit, are expressed by various artists. Immortal Technique, who is an independent rapper and has started his career without the help of music industry has said that ´ *They want us to just dance and sing and smile and pretend that the world is ok. They believe hip-hop is sheer entertainment. Entertainment can be used for many things: to inspire and educate but also to pacify, to keep people stupid and preoccupied with things that aren't important.*´[139] Similarly to the example from history where the publishers had the control and power of distribution, internet allows the return of the copyright to its real owners, the artists. Furthermore, it can be claimed

[139] O. Shahid, *Interview with Immortal Technique,* The Guardian, 25 October 2012.

that the current copyright laws actually intervene with the right to privacy in itself, if it is built for the protection of ´legal´ holders of copyright, such as representatives of artists when the artists have resigned their rights in order to be able to share their work. When in the past copying music (for example, copying music from CD) had its consequences on the quality of the sound, then digitalization allows creation of copies with exactly the same quality. *´As information is digitalised, it is approximated as a discreet set of its parts. Each measurement is a sample representing the sound at a particular (and very short) moment in time.´*[140] Hence, copying does not carry with itself any penalties. This makes the owners of the copyright fear that people copy without paying, especially as distribution is at ease due to internet. If previously the suffering of the quality after copying was a barrier to massive replication, then now the incentives for authorized copying are lowered.[141] Furthermore, *´the future-proof foundation of the internet as a global digital network means that it has not had to be abandoned, replaced, or even fundamentally altered to make possible instant sharing.´*[142] It is reasonable to expect that people start utilizing the power of digitalisation and internet. Especially, as the prices of reproduction have decreased radically, the old business models for distributing creative work are no more acceptable if one has to pay the same price for a piece of music as he did before the era of digitalisation.

The rapid development of new forms of digital information technology has made sharing and accessing files online in revolutionarily easy manner. One of the ways this is done is via peer-to-peer (P2P) networks. These types of file sharing networks are not illegal in itself, as the initial purpose of these is to encourage and give opportunity to people to share files which they own the intellectual property right to. However, it also allows sharing of any other files (music, films, games etc.) without authorized right. Modern P2P networks are *´communication structures that allow a network of personal computers with the same networking program to connect with each other, and directly*

[140] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 54.
[141] *Ibidem*, p. 60.
[142] *Ibidem*, p. 59.

*access and share files from one another's hard drives.'*[143] The incentive for downloading copyright material for free is increasing every year. However, what distinguishes P2P networks from other forms of acquiring free files is that the individuals, who are downloading, are automatically uploading the files from their shared folder in their hard drives. This also makes them potential infringers of copyright as they are sharing without a permission to do so. The scope of the problem as identified by Recording Industry Association of America (RIAA) is as follows[144]:

- From 2004 through 2009 alone, approximately 30 billion songs were illegally downloaded on file-sharing networks.
- NPD reports that only 37 per cent of music acquired by U.S. consumers in 2009 was paid for.
- Digital storage locker downloads constitute 7 per cent of all Internet traffic, while 91 per cent of the links found on them were for copyrighted material, and 10 per cent of those links were to music specifically.[145]

This assessment has some implications that cannot be ignored when talking about the protection of copyright online. First, the number of internet users that are downloading illegal material is rising every year. These statistics are only showing the numbers in music industry and not including any video material, which would increase the number of downloads vastly. In addition, it only includes downloads that have been identified and excludes accessing copyrighted material online (for example, video material that can be watched free online via streaming). There is an indication of lack of initiative of users to pay for copyrighted material. In addition, free downloading is not the only initiative for usage of P2P networks.

[143] C. Deschamps, *Peer-to-peer (P2P) networks and copyright law in France*, *Ireland and the UK*, Irish Student Law Review, 2010, p. 157.
[144] RIAA is the trade organization that supports and promotes the creative and financial vitality of the major music companies. Its members are the music labels that comprise the most vibrant record industry in the world. RIAA® members create, manufacture and/or distribute approximately 85% of all legitimate recorded music produced and sold in the United States, for more: http://www.riaa.com/aboutus.php?content_selector=about-who-we-are-riaa
[145] RIAA, Piracy Online: Scope of the Problem, 2013.

However, as copyright can be viewed as a form of right to privacy and application of it as an enforcement of private rights in public domain, various human rights considerations arise. File sharing networks can also have positive impacts to the society as a whole. It encourages technological innovation and enables production and distribution of educational and political materials (for instance documentaries) that otherwise would not have been produced.[146] *´Peer-to-peer platforms reconstruct social control over the means of distributing and informational good.´*[147]It has the potential to shift the power of knowledge from traditional media to the people. Everyone can serve the role of being a public watchdog, if only they are empowered to do so. In addition, *´another example is the long-term cultural impacts that exposure to diverse creative materials might have on individuals. More generally, peer-to-peer fire-sharing platforms cover a very wide range of autonomy-based social benefits that serve free speech values with regard to both speakers and recipients of content and information.*[148] It must be noted that the human right considerations that arise with copyright and P2P networks are deeply rooted in personal autonomy, which in itself affects the development of identity. These concerns, hence, return to privacy issues, which must be balanced with the rights of others and ´necessary in democratic society´. To assess the balancing of rights in peer-to-peer networks, two opposite policies of copyright enforcement will be compared. The French approach illustrates the wide spread view of copyright infringement as theft and a criminal act. Canada, on the other hand, has adopted methods of enforcement whereby copyright is not exclusive right and must be balanced with concerns of online privacy.

[146] G. Pessach, *An international-comparative perspective on peer-to-peer file-sharing and third party liability in copyright law: framing the past, present and the next genreations´ questions*, Vanderbilt Journal of Transnational Law, 2007, p. 106.
[147] *Ibidem*, p. 111.
[148] *Ibidem.*

4.4. French HADOPI laws: history, specificity and implications.

Since 2001 the European Commission h.as passed two main legislative documents on protection of copyright in European Union. First on 22 May 2001 it passed a directive on the harmonisation of certain aspects of copyright and related rights in the information society (commonly referred to as INFOSOC Directive).[149] In the preamble it takes the position of creation for the purposes of monetary return. It states that ´*If authors or performers are to continue their creative and artistic work, they have to receive an appropriate reward for the use of their work, as must producers in order to be able to finance this work. Adequate legal protection of intellectual property rights is necessary in order to guarantee the availability of such a reward and provide the opportunity for satisfactory returns on this investment*.´[150] The second Directive, passed on 2 June 2004, concerns the harmonisation of copyright enforcement in its member states (IPRED).[151] In addition to harmonisation within member states, it aims to create a common framework that is compatible with international copyright laws, especially the Agreement on trade-related aspects of intellectual property (TRIPS Agreement). ´ *The TRIPS Agreement contains, in particular, provisions on the means of enforcing intellectual property rights, which are common standards applicable at international level and implemented in all Member States*.´[152] The bill for adoption of HADOPI (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet)* law was submitted to French Parliament in 2005 after the Government received a warning from European Commission for not adopting measures to comply with INFOSOC Directive.[153] Furthermore, it follows a French Code of Intellectual Property, which states that ´*any copying of a work without the consent of its author, whether in whole or in part, including illegal file sharing activities, constitutes and infringement of the*

[149] Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society, 22 May 2001.
[150] *Ibidem*, Preamble, §10.
[151] Directive 2004/48/EC of the European Parliament and of the Council, 29 April 2004, on the enforcement of intellectual property rights.
[152] *Ibidem*, Preamble, §5.
[153] Y. Breindl and F. Briatte, *Digital network repertoirs and the contentious politics of digital copyright in France and the European Union,* Internet, Conference on Politics, Policy: An Impact Assessment, Oxford Internet Institute, 16-17 September 2010, p. 10.

*author's exclusive right to reproduction.'*[154] HADOPI Law is based on a three-warning system for which France was the first country to adopt such measures to enforce the protection of copyright in P2P networks.[155] It functions in the manner where first rights owner identifies the infringement of copyright and informs Hadopi (High Authority for the Diffusion of Works and the Protection of Copyright on the Internet), which then verifies the infringement. Hadopi then turns to internet service providers who keep control over and track the suspected content-sharers. In addition, to the direct claims from copyright owners, it is the task of the Hadopi Authority to monitor the internet in order to determine perpetrators of illegal download (as they are the individuals who also share the content in the same time). When the infringement and the culprits are identified, the first warning via e-mail is sent directly by the service providers. Three e-mail warnings must be sent before the official judicial complaint is submitted. If the infringement continues after third e-mail, then the judge has a power to impose penalties, such as disconnection of internet for a period ranging from two to twelve months.[156] The appeal against disconnecting is only allowed after the sanction has been ordered and it does not allow full reconnection, but only a reduction in time.[157] Disconnection from internet, as a punishment, illustrates the modern forms of criminal justice. Imprisonment as a punishment has been used to denounce liberties of individuals after they have abused their freedom. In internet, as a separate realm, allows people the freedom to access and share information along other benefits that it brings with it (economic, access to state etc.). However, freedom goes hand-in-hand with responsibilities, as also noted by the Court. Disconnecting someone from internet, therefore, can be seen as a new form of punishment as it takes away the liberties that law abiding citizens have. In addition, as internet is a new reality, such a punishment can be considered equal to imprisonment that is supposedly protecting the rights of others by removing the delinquents from the society – in this case the virtual society.

---

[154] C. Deschamps, *Peer-to-peer (P2P) networks and copyright law in France, Ireland and the UK*, Irish Student Law Review, 2010,p. 162.
[155] N. Lucchi, *Regulation and Control of Communication: The French Online Copyright Infringement Law (HADOPI)*, Max Planck Institute for Intellectual Property and Competition Law Research Paper No. 11-07, 2010, p. 5.
[156] *Ibidem.*
[157] *Ibidem*, p. 7.

Furthermore, the criminalisation of copyright infringement is established by Article L-335-2 of French Intellectual Property Code, whereby ´Infringement in France of works published in France or abroad shall be liable to a three-year imprisonment and a fine of € 300.000.´[158]

The first version of HADOPI allowed the created Authority to impose sanctions after monitoring and sending warnings to the alleged violators. This gave Hadopi Authority power that exceeds its legitimate mandate. Hence, it also undermined the right to fair trial. *´On the one hand, the creation of this administrative control Authority found its justification in the necessity to safeguard copyright which is directly threatened by the advent of digital technologies; but on the other hand it was likely to collapse or weaken those constitutional guarantees designed to preserve constitutional freedoms and liberties.´*[159] The original Hadopi was changed because it was found by the Court to be conflicting the presumption of innocence granted by the French Constitution.[160] The new Hadopi 2 returns the power of sanctioning to courts and leaves the duties of the Authority to be monitoring and warning. However, it resolves the presumption of innocence problem only to an extent. Monitoring in order discover illegal downloads, requires some form of knowledge of the content that has been downloaded. If and extensive database, related to private information (such, as internet protocol), comes to existence by monitoring ´public space´, possible issues of privacy arise.[161]

The process of monitoring, as such, takes the form of surveillance. Surveillance itself can undermine the presumption of innocence. Problems of surveillance arise mainly if it is carried out in secret. However, in internet it has similar effect if every action online is visible and, hence, only ´monitored´. The virtual reality, as explained in precious chapters, does not allow presumption of consent - to be watched - of the people who enter cyberspace. This form of online surveillance, under the umbrella term of monitoring, is a potential threat to privacy and freedom from arbitrary interference. If the right to privacy and presumption of innocence are undermined by online

[158] Article L-335-2, French Intellectual Property Code, 1 July 1992.
[159] N. Lucchi, *Regulation and Control of Communication: The French Online Copyright Infringement Law (HADOPI)*, Max Planck Institute for Intellectual Property and Competition Law Research Paper No. 11-07, 2010, p. 11.
[160] Intellectual Property Watch, Hadopi 2 Passes French Senate, 9 July 2009.
[161] As explained by the European Court of Human Rights in the case of *P.G and J.H.*

surveillance, then a society of mistrust is created. Firstly, the state positions itself in a superior position as it becomes obvious that it does not trust its own people. Secondly, the people who feel mistrusted become sceptical of the state. In addition, this creates a chilling effect on the usage of internet and sharing of knowledge that does not infringe copyright. It effectively illustrates why top-down approach to balancing online copyright and privacy, is ineffective. ´*Nowadays peer-to-peer information sharing has become such a widespread phenomenon; broadband users simply expect their providers not to constrain their information sharing behaviour.*[162]

Surveillance is allowed only if it protects democratic institutions. One feature of it is the pressing social need, as explained in above paragraph. However, protection of democratic institutions also requires the upholding of the principles that democracies are built up on. These features are the rule of law, which requires coherent legal principles that can be accessible to individuals. These legal doctrines are based on certain ethics created by legal theories. The approach to balancing that the Courts take must be between the right to privacy and surveillance that protects democratic societies.

Offline intellectual property likely is in a form of tangible objects, such as books, DVDs and CDs. This falls under traditional property law and the crime of theft. Offline copyright infringement is likely to serve a purpose of profit, hence directly infringing the right for remuneration of the authors. It is unlikely, that someone makes an effort and expense to copy and store material without an expectation of profit. Especially, as one has to go to physical public place to distribute the copies. This is where the first copyright laws originate. The purpose has been to protect copyright holders from competing commercial actors, who are exploiting the property of the rights holders.[163] However, in digital and online world, storing and sharing becomes effortless and quick. Hence, the initiatives for copying and sharing for free and for private purposes are increased. Therefore, traditional copyright laws are outdated as its principles cannot be applied to cyberspace. The Court of Human Rights has to balance the right to privacy that arises from the monitoring of contents that are not meant for the purposes of profit. The interference is acceptable if it is prescribed by law. Copyright enforcement in the

[162] V. Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, p. 84.
[163] G. S. Moohr, *The crime of copyright infringement: an inquiry based on morality, harm, and criminal theory,*Boston University Law Review, 2003, p. 741.

form of criminalisation undermines the legality of the laws and affects the principle of necessary in democratic society.

Two main philosophical approaches of criminal law and punishment establish the legitimacy of the laws. First, the retributivists argue that conduct should be treated criminal if it is morally wrong. The formation and meaning of morality extend beyond the current analysis, but one is evident: the morality in democratic societies depends on the moral views of the individuals. Hence, the retributivist theory is inapplicable due to the extent of individuals that are using peer-to-peer networks and collectively not perceiving it as an immoral act. Only during the year 2012 there were 613,271 first strike warnings sent by e-mail.[164] Yet, surveys indicate that more than half of those polled, do not see downloading music as immoral.[165] The second philosophical approach to crime is the consequentialism that focuses on the authority to criminalise if the purpose is to maximise the social welfare or harm prevention.[166] The harm in copyright is seen as harm to the integrity of the copyright holders by depriving their right their intellectual property. First, the calculations of loss of profit due to peer-to-peer systems do not reflect the reality. It is nearly impossible to prove that the person who downloaded something for free would have actually purchased it otherwise. Secondly, it can be argued that social harm arises as the incentives to create are decreased. However, the dimensions of cyberspace change the business model of distributing work. Internet allows authors to make their work accessible to the public directly. *´Direct distribution of creative work over the internet could stimulate innovators to create more, not less, material, and make legal prohibitions less important in the artistic calculation. Technology and market forces may thus provide an incentive to create, making it unnecessary to rely so heavily on legal devices, such as criminal copyright laws, to motivate innovation.´*[167]

The harm principle requires that the harm must implicate some interest of the wider society. In addition, it requires that it does not create greater harms than it prevents.[168]

[164] World Intellectual Property Review, Hadopi Strikes at the Heart of Online Piracy, 24 January 2013.
[165] G. S. Moohr, *The crime of copyright infringement: an inquiry based on morality, harm, and criminal theory*, Boston University Law Review, 2003, p. 767.
[166] *Ibidem*, p. 749.
[167] *Ibidem*, p. 749.
[168] *Ibidem*, p. 753.

Surveillance as a method for copyright enforcement creates greater harms than it attempts to prevent. It could be allowed in cases of crime prevention if it does not undermine democratic values. However, if criminal law is built up in ignorance towards the consensus of people, it becomes nearly impossible to enforce. If it opposes the moral values of the general society, then the people lose respect for laws and this undermines the legitimacy of the laws. Furthermore, attempting to enforce certain morals upon the society, through criminalisation, is not desirable in upholding of democratic values. If the morals are created top-down then the society becomes oppressed rather than sincerely valuing the legislation.[169]

4.5. Canadian Copyright Act 1921: history, specificity and implications.

Canada has adopted a different approach to tackle the problem of file sharing on peer-to-peer networks. Canadian Copyright Act 1921 was amended in 1997 whereby copying for private interest was legalised and remuneration for copyrighted works is granted through a system of levies. Article 80 allows copying for the purpose of private use:

(1) the act of reproducing all or any substantial part of

(a) a musical work embodied in a sound recording,

(b) a performer's performance of a musical work embodied in a sound recording, or

(c) a sound recording in which a musical work, or a performer's performance of a musical work, is embodied onto an audio recording medium for the private use of the person who makes the copy does not constitute an infringement of the copyright in the musical work, the performer's performance or the sound recording.[170]

Article 82 puts an obligation on all manufacturers and importers of blank audio media sold in Canada to pay levy:

[169] *Ibidem*, pp. 774-778.
[170] Article 80(1)(a)(b)(c) Canadian Copyright Act 1921.

(1) Every person who, for the purpose of trade, manufactures a blank audio recording medium in Canada or imports a blank audio recording medium into Canada

(a) is to pay a levy to the collecting body on selling or otherwise disposing of those blank audio recording media in Canada.[171]

However, neither of these articles implies that copyright infringement is not followed by criminal liability. In fact, article 42 establishes criminal liability of:

(1) Every person who knowingly

(a) makes as sale or rental an infringing copy of work,

(b) sells or rents out, or by way of trade exposes or offers for sale or rental, an infringing copy of a work,

(c) distributes infringing copies of a work either for the purpose of trade or to such an extent as to affect prejudicially the owner of copyright.[172]

The Act creates some problems of interpretation as Article 42 (1)(c) establishes liability for infringement if the work that is distributed to the extent that prejudicially affects the owner of copyright. It can be argued that the extent of free distribution on peer-to-peer networks has the potential to create financial harm and harm to the integrity of copyright holders. In addition, Article 3 requires authorization for production and reproduction of copyrighted works, which means that the original distributer must obtain the authorization for distribution. These questions have been dealt with by the Federal Court of Canada and the Federal Court of Appeal in the case of *BMG Canada Inc. v John Doe.*[173] In this case, the Canadian Recording Industry Association brought an action against five internet service providers in Canada, in order for them to disclose the identities of twenty-nine end-users of peer-to-peer networks. The requirement for the disclosure of the identities was that the applicant must establish a *prima facie* case in

[171] Article 82(1)(a) Canadian Copyright Act 1921.
[172] Article 42 (1) (a),(b), (c) Canadian Copyright Act 1921.
[173] *BMG Canada Inc. v. John Doe*, 2004 FC 488, [2004] 3 FCR 241.

terms that the infringement of copyright had taken place.[174] The Federal Court established that, under Article 80(1), downloading a song for private use does not constitute an infringement.[175] It was argued that the infringement took place in terms of ´authorization´ of the shared material. However this argument was rejected by the Court that placed its authority on the case of *CCH Canadian Ltd. v. Law Society of Upper Canada*, which established that there setting up establishments that allow copying does not amount to authorizing infringement.[176]The Court added that there is no *´real difference between a library that places a photocopy machine in a room full of copyrighted material and a computer user that places a personal copy on a shared directory linked to a P2P service. In either case the preconditions to copying and infringement are set up but the element of authorization is missing´*.[177] Furthermore, it was noted that the Court should presume that the authorization has taken place in accordance with law, unless there is evidence that certain degree of control existed between the alleged authorizer and the persons who committed the infringement. Hence, that there must exist a certain degree of intent to infringe the requirement of authorization.

The manner, in which the Court dealt with the issues of distribution, also lead to a finding that no infringement of copyright took place. For the infringement to uphold there must be a positive and intentional act for the purposes of distribution:

*´The mere fact of placing a copy on a shared directory in a computer where that copy can be accessed via a P2P service does not amount to distribution. Before it constitutes distribution, there must be a positive act by the owner of the shared directory, such as sending out the copies or advertising that they are available for copying. No such evidence was presented by the plaintiffs in this case. They merely presented evidence that the alleged infringers made copies available on their shared drives.´*[178]

---

[174]G. Pessach, *An international-comparative perspective on peer-to-peer file-sharing and third party liability in copyright law: framing the past, present and the next genreations´ questions*, Vanderbilt Journal of Transnational Law, 2007, p. 102.
[175] *BMG Canada Inc. v. John Doe*, 2004 FC 488, [2004] 3 FCR 241, §8.
[176] *CCH Canadian Limited v. Law Society of Upper Canada*, [2004] 1 SCR 339,[1] 2004 SCC 13.
[177] *BMG Canada Inc. v. John Doe*, 2004 FC 488, [2004] 3 FCR 241, §27.
[178] *Ibidem*, §28.

In addition, the Court brought up privacy concerns that disclosure of identities would give arise to. It noted that, the right to privacy cannot be used as a shield against civil or criminal liability and that it must be assessed in relation to the public interest that the copyright (or any other opposing right) entails. The Court ruled that the privacy interest outweighed the public interest because the extensive time laps between the gathering of evidence and the request for disclosure.[179] The unjustified lapse of time *´clearly makes the information more difficult to obtain, if it can be obtained at all, and decreases its reliability´.*[180] Even, though the Court takes a mere procedural position for its judgement, it refers to the etiquette developed in the usage of internet, whereby keeping the identity of internet protocol address private in some degree, is a good public policy. The explanation behind this is the social contract created between internet service providers and the users. On one hand, the service providers safeguard user's privacy, while the users agree to behave according to certain norms, such as transmitting defamatory or libellous messages.[181]

The decision was appealed by the record companies to the Federal Court of Appeal. Judge Sexton J.A. of the Court of Appeal criticised the findings of the Federal Court. He pointed out few flaws of the initial judgement. Firstly the point that *´if the users were not using an "audio recording medium", the defence of private copying would not be available,´* was not considered by the Federal Court.[182] Secondly, the failure to consider *´whether the users' act of copying the songs onto their shared directory could constitute authorization because it invited and permitted other persons with Internet access to have the musical works communicated to them and be copied by them.´*[183] Thirdly, he criticised the fact that the Judge in the Federal Court relied on the requirement of positive act for establishing ´distribution´, which is not clearly stated by the legislation or relevant authority.[184] Finally, in relation to *mens rea,* Judge Sexton J.A. raised a valid point on intention where the defendant should or ought to have

[179] *Ibidem,* §5.
[180] *Ibidem,* §37.
[181] *Ibidem.*
[182] *BMG Canada Inc. v. John Doe,* 2005 FCA 193, [2005] 4 RCF 81, *§50.*
[183] *Ibidem,* §51.
[184] *Ibidem,* §52.

known that infringement took place (requirement of foreseeability for criminal intent).[185] Even though, the Court of Appeal pointed out that the assessment on infringement can be argued for both ways and in this case the potential for finding interference in high, it does not really play a role in making a difference in the outcome. The appeal was dismissed on the basis of concerns for privacy. Furthermore, the Court of Appeal noted that the Federal Court was mistaken in its approach to assess primarily the issues copyright infringement, as the case itself is concerned with disclosure of identities of people who use peer-to-peer networks, hence a case of privacy.

The Court of Appeal notes that the development of technologies and internet should not undermine other rights, such as copyright, that the society has deemed valuable.[186] It also agrees with the Federal Court on the point that if too much time has elapsed between the collection of information and the request for the identities, it imposes a threat that *´innocent persons would be infringed and legal proceedings against such persons would be without justification´*. However, the Court of Appeal emphasises that only if the claimants have a *bona fide* claim against the infringers, they have a right to request the identification for the purposes of bringing legal actions. *Bona fide* also requires that no private information irrelevant to the copyright issues in extracted by the plaintiffs during the investigation. *´If private information irrelevant to the copyright issues is extracted, and disclosure of the user's identity is made, the recipient of the information may then be in possession of highly confidential information about the user. If this information is unrelated to copyright infringement, this would be an unjustified intrusion into the rights of the user.´*[187] The final judgement of dismissing the case, based on this justification, has a broader implication on the ways in which the Court will deal with similar cases in the future. It is evident, that the courts in Canada would rather abstain from judging on future claims on copyright infringement on peer-to-peer networks because of the extent and difficulty of balancing it imposes. It is very difficult for copyright holders to obtain information only related to the infringement, as any mean of surveillance or data gathering would most likely reveal other information about

[185] *Ibidem*, §53.
[186] *Ibidem*, §41.
[187] *Ibidem*, §44.

the user. Furthermore, because of the difficulty to gather data the copyright holders are more likely to target the ´original´ uploaders rather than the chain of people that follow it. This does not make sharing of copyrighted material legal, but it creates a loophole whereby it becomes legal for the every-day users of peer-to-peer networks. It also upholds the finding of the Federal Court, whereby sharing copyrighted material in the P2P networks does not constitute an infringement, as it is for the purpose of private use.

To uphold the right of the creators to their work Canadian Copyright Act also includes the right to remuneration via the system of levies. It has been proposed by William Fisher that:

*´The enforcement of copyright with regard to peer-to-peer file sharing platforms should be enforced ex-post through a system of mandatory levies that would come together with a statutory exemption for private and non-commercial copying of copyrighted materials through peer-to-peer file-sharing platforms. Such a scheme would function as a form of blanket compulsory license, authorizing copying under a specific exemption for private and non-commercial copying, in exchange for set fees that would be allocated between copyright owners.´*[188] This type of levy system can, on one hand, deal with the economic or reputational losses that the peer-to-peer networks threaten to create. Furthermore it can encourage creativity as it becomes easy for anyone to share his or her works.

The Canadian approach solves the problems of criminalisation of copying for private purposes. It also presents a solution to mass surveillance. The Court has taken a clear position that the methods of investigation by the plaintiffs must be subject to restrictions in order to safeguard privacy. It does not only make a statement, but also suggests practical means of achieving it. It says that *´only the internet pseudonyms appear as defendants in the statement of claim. A confidential annex would have been added to the statement of claim relating each pseudonym to the name and address of an ISP account holder. Finally, the ISPs would not have been required to provide affidavits in support*

[188] G. Pessach, *An international-comparative perspective on peer-to-peer file-sharing and third party liability in copyright law: framing the past, present and the next genreations´ questions*, Vanderbilt Journal of Transnational Law, 2007, p. 100.

*of their findings.'*[189] However, the Canadian approach creates two main concerns. Firstly, it eliminates the expenses of public budget, as it does not incorporate enforcement by public authorities. The difficulties that make it expensive and time consuming to retrieve data are outlined as:

- *'such information routinely kept by the ISPs but information that must be specifically retrieved from their data banks;*
- *the older the information is, the more difficult it will be to retrieve it;*
- *the older the information, the more unreliable the result that will be produced;*
- *it may be impossible, due to the passage of time, to link some IP addresses to account holders;*
- *at best the ISPs will generate the name of the account holders; however, they can never generate the name of the actual computer users. An IP address, for instance, can lead to the name of an account holder, but that account holder could be an institution and/or may be linked to a local area network of many users.'*[190]

The expenses following this process are placed upon the copyright users. Hence, it can be argued that it becomes burden on copyright holders when enforcing their rights. The second concern of the Canadian copyright law and the case of *BGM Canada*, is that it has potential to undermine the rule of law in terms of accessibility and foreseeability. Even though it creates a legitimacy of downloading for private purposes, it the tests and the possible approach of the Court in the future, remains unclear. It can be considered that the decision by the Federal Court in terms of peer-to-peer networks upholds because the appeal was dismissed. However, it was upheld due to the failure of the claimants to follow the ethics of internet on data retention after passage of time. Hence, it is difficult to predict whether the position of the court upholds when procedures are followed correctly. Especially, as the Court of Appeals did not agree, on the point of law, with the assessment of the Federal Court in terms of what constitutes authorization

[189] *BMG Canada Inc. v. John Doe*, 2005 FCA 193, [2005] 4 RCF 81, §5.
[190] *BMG Canada Inc. v. John Doe*, 2005 FCA 193, [2005] 4 RCF 81, §34.

and intention to distribute. This makes the law of Copyright vague and undermines to principles of accessibility and foreseeability of the rule of law. It is evident that the Canadian approach, in its current form, is not the most desirable way. However, it does illustrate how the laws of copyright have been adopted to digital age. It acknowledges that outdated principles of law enforcement can be a threat to the progress of the societies. It also attempts to respond to the public pressure instead of directly enforcing morals of behaviour through surveillance, as required by full criminalization of copying. By allowing copying for private use and criminalizing it only if it is done for purposes of profit, the mass surveillance is decreased.

## 4.6. Conclusion.

Enforcement of copyright illustrates how application of traditional theories and laws are not effective when applied to new means of communication technology. It can be a burden for both, the owners of copyright and the society as a whole. Criminalisation and enforcement of it through public financing becomes a burden to a society. Furthermore, due to the pressing social need and the gravity of usage of peer-to-peer networks, criminalisation becomes arbitrary and loses its legitimacy. It constitutes interference to privacy as it increases the online sensitivity as it interferes with individual´s behaviour. People are not even aware of the amount and type of data that is stored about them (at least the extent of it). One would not consider private ´Google search´ public. Hence, criminalising and the means of enforcement of copyright laws (the crawlers; robots; trackers) are intervening with privacy because it is interference with actions that people themselves still consider private. Before any law enforcement or trying to protect people´s privacy, it should be considered what people consider private according to their behaviour. The behaviour implies the reasonable expectation of privacy that has be emphasised valuable by the Court. By educating people about the dangers of them being monitored online and raising awareness before legislation, being subjected to monitoring becomes a willing act that assumes consent. However, the gravity of usage of peer-to-peer networks emphasises the expectation of people, who do not see downloading copyrighted material as immoral. This aspect has been dealt with the Canadian approach. It is not the perfect balancing of rights as it imposes greater burden

on copyright holders. Furthermore, the Canadian courts do not sufficiently eliminate the problems of ambiguity of the legislation, which undermines the principle of rule of law. However, the Canadian approach is one of the positives steps in terms of acknowledging that the laws of copyright enforcement must be effectively adjusted to virtual reality.

## CONCLUSIONS

Privacy is always relative to its exposure to public intervention. The method that has been adopted to distinguish between private and public looks at the means of gathering data. For instance, surveillance requires legitimate procedures and purpose in order to be ´in accordance with law´. The cases of *P.G. and J.H* and *Peck* establish two ways in which privacy can be intervened with in public spaces. Firstly, private life considerations arise when permanent record of persons and their private characteristics come into existence. Secondly, even in public, individuals have reasonable expectation of privacy. Reasonable expectation becomes the most valuable and significant feature when defining what is private and how it can be intervened in. Modern liberal democracies are based on individual autonomy. Autonomy will be undermined if privacy will not be considered according to the expectations of individuals. Of course, the freedom requires some form of responsibilities, but only if people know what is expected from them. However, technological developments, especially in the field of information and communication technology, change the distinction and definition of privacy.

With the creation of World Wide Web marked the beginning of internet revolution. It increased user-friendliness making the networked information accessible to general public. When such a powerful tool for creation, access and exchange of knowledge reaches to the people, then the progress of the societies takes a new discourse. Internet serves equally important purposes in the social, economic and public spheres of people´s lives. It becomes so essential for functioning of modern societies that it becomes a new reality and space for life to happen. With the rise of social media internet allows individuals to communicate with no limits of space or time. Individuals

can easily share information between each other and enforce their right to maintain and establish relationships at ease. Social space becomes reality due to variety of experience that people subtract from the social media. It creates a new space for integration as people can exist in the same space while physically being apart. The effect of internet varies depending on individual circumstances. It can create emotions of loneliness or courage, depending on past and present experiences. It is unlikely that people experience cyberspace the same way, as it is unlikely that everyone has the same life experience. For instance, elderly have more difficulties in adapting to internet communication because they have to change their old ways. The internet generation, however, do not have to adapt as they are already born into the network society. In addition, social space allows presenting oneself with a completely different identity than in offline space. Internet allows individuals to globally reach businesses and vice versa. Whether the impact of it to job market is positive or negative can be debated. However, it is clear that it impacts it in ways that directly affect people´s welfare. The economic impact that affects the way people experience life. Cyberspace influences the shift of traditional models of business and free market. Sharing of information and knowledge becomes the main economic activity and allows the creation of shared memories and collective intelligence. The new models of sharing knowledge affect the relationship between citizens and the state. Traditional profit orientated journalism is overthrown by public who take a new role of being public watchdogs. Cyberspace has the potential to encourage democracies as it increases public participation in the matters of the state. Because the gravity of impact of cyberspace on everyday life is so great, it creates a completely new space and virtual reality. New reality causes the shift of reasonable expectation of privacy and old rules cannot be applied to new space.

Privacy in cyberspace is relative to what is considered public. No individual would consciously think about privacy, unless some information has become private due to public interaction. Cyberspace cannot be defines as one space. It can be difficult to establish the reasonable expectations of privacy online in a way that is applicable to everyone. Cyberspace places individual´s information under greater public scrutiny, and people would consciously have to think about every action they perform online.

However, as the Internet becomes a new reality, this would not be the most desirable way to operate it. The example of Stacy Snyder illustrates how the legal protection of privacy is out-of-dated. More importantly, it is an example of how the prejudice in the society becomes a problem in terms of online privacy. The widespread theory that knowledge is power creates a technological dependence of internet that empowers individuals. However, the power of knowledge is shifted with the creation of big data. Similar freedoms must be allowed in virtual reality as in offline world. Gathering and storing a mass of data becomes a problem if it is done in a systematic manner and takes a form of surveillance. Firstly, surveillance can be used as a form of social control by the state and by big businesses. Secondly, surveillance intervenes with individual´s privacy due to its power to shape autonomous choices and behaviour. Policies of covert surveillance create a culture of distrust and control. However, the global society of legal thinkers has talked about the new right to forget online. This aims at shifting the control over information from states and corporations back to individuals. It becomes essential because people are unaware of the extent of information that is available about them online. The right to forget has also been emphasised by the European Commission. However, the main concern of the proposed regulation is that it does not fully deal with all the privacy problems that arise in cyberspace. For instance, it does not take into account the consequences of increased prejudice, such as, in the case of Stacy Snyder. The European Court of Human Rights and Council of Europe have also recognised privacy problems only to an extent. They have pointed out problems of privacy, such as storage of data, surveillance and general threats of being visible online. However, not enough cases on online privacy have reached the Court, in order to have fully developed protection of online privacy in Europe. The problems of privacy in cyberspace reach far beyond what has been established by the current legislation in Europe. This can be seen in the case of copyright enforcement, which arises much bigger concerns regarding the chosen policies for governing European countries.

Enforcement of copyright illustrates how application of traditional theories and laws are not effective when applied to new means of communication technology. It can be a burden for both, the owners of copyright and the society as a whole. Criminalisation and

enforcement of it through public financing becomes a burden to a society. It can be argued that Moore´s law and rapid advancements in communications technology allow the ´race´ between the state and ´criminals´. For instance, online proxies and encryptions can increase anonymity online and enable individuals to ´hide´ from monitoring, surveillance and interference with privacy. On one hand, this can encourage the technological advancements, as the state will make a greater effort to break through these systems and the individuals will make a greater effort to beat the technology of the state. However, this has variety of policy concerns and one of them being, not being able to construct coherent legislation.

Furthermore, due to the pressing social need and the gravity of usage of peer-to-peer networks, criminalisation becomes arbitrary and loses its legitimacy. It constitutes interference to privacy as it increases the online sensitivity as it interferes with individual´s behaviour. People are not even aware of the amount and type of data that is stored about them (at least the extent of it). One would not consider private ´Google search´ public. Hence, criminalising and the means of enforcement of copyright laws (the crawlers; robots; trackers) are intervening with privacy because it is interference with actions that people themselves still consider private. Before any law enforcement or trying to protect people´s privacy, it should be considered what people consider private according to their behaviour. The behaviour implies the reasonable expectation of privacy that has be emphasised valuable by the Court. By educating people about the dangers of them being monitored online and raising awareness before legislation, being subjected to monitoring becomes a willing act that assumes consent. However, the gravity of usage of peer-to-peer networks emphasises the expectation of people, who do not see downloading copyrighted material as immoral. This aspect has been dealt with the Canadian approach. It is not the perfect balancing of rights as it imposes greater burden on copyright holders. Furthermore, the Canadian courts do not sufficiently eliminate the problems of ambiguity of the legislation, which undermines the principle of rule of law. However, the Canadian approach is one of the positives steps in terms of acknowledging that the laws of copyright enforcement must be effectively adjusted to virtual reality. Copyright enforcement raises specific concerns about privacy in terms of

power of controlling personal information. Current methods of copyright enforcement highlight various human rights problems because of the failure to adapt the specificities of cyberspace into the process of balancing rights. The main concern arises in terms of reasonable expectation of privacy that requires adjusting policies according to how individuals perceive privacy online. This also raises the concern of to what extent are the morals of individuals the basis for regulation and to what extent certain policies impose morals upon the society, hence, intervene with individual´s autonomy and freedom of conscience. Finally, the cyberspace has shifted the traditional models of business and economy. It is evident, that currently copyright laws follow the traditional models of business and profit. However, these dimensions are radically changed by the open access of cyberspace. Hence, the future of right to privacy is in the hands of the great masterminds of economists. Only by adjusting business models according to virtual reality, the appropriate legislation in the field will follow.

## BIBLIOGRAPHY


Arthur, W. B. (2011). The secon economy. *Internet Matters: Essays in Digital Transfrormation*, 206-212. McKinsey Global Institute.

Breindl, Y., & Briatte, F. (2010). Digital network repertoirs and the contentious politics of digital copyright in France and the European Union. *Politics, Policy: An Impact Assessment* (lk 1-35). Oxford: Oxford Internet Institute.

Bughin, J., & Manyika, J. (May 2011. a.). The macroeconomic impact of the Internet. *Internet Matters: Essays in Digital Transformation*, 2-37. McKinsey Global Institute.

Castells, M. (2001). *The Internet Galaxy.* New York: Oxford University Press Inc. .

Commission, E. (2012). *Digital Agenda Scoreboard 2012*. Kasutamise kuupäev: 25. June 2013. a., allikas Digital Agenda for Europe: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/scoreboard_life_online.pdf

Conen, P. (1952). Aristotle´s definition of time. *The New Scholasticism, 26*(4), 441-458.

Council of Europe. (4. April 2012. a.). Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the Protection of Human Rights with Regard to Social Networking Services.

Council of Europe. (11. June 2013. a.). Declaration of the Committee of Ministers on Risks to Fundamental Rights Stemming from Digital Tracking and Surveillance Technologies.

Deschamps, C. (2010). Peer-to-peer (P2P) networks and copyright law in France, Ireland and the UK. *Irish Student Law Review, 17*, 155-186.

Dijk, J. v. (2006). *The Network Society: 2nd Edition.* London: SAGE Publications Ltd.

Dinev, T., Hart, P., & Mullen, M. (2008). Internet privacy concerns and beliefs about government surveillance - an emperical investigation. *Journal of Strategic Information Systems, 17*(3), 214-233.

Europe, C. o. (4. April 2012. a.). *Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines*. Kasutamise kuupäev: 25. June 2013. a., allikas Council of Europe: Committee of Ministers: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CM%20Rec(2012)3%20E%20-%20Search%20engins.pdf

Europe, C. o. (4. April 2012. a.). *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*. Kasutamise kuupäev: 25. June 2013. a., allikas Council of Europe: Committee of Ministers: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/CM%20Rec(2012)4_En_Social%20networking%20services.pdf

Europe, C. o. (11. June 2013. a.). *Declaration of the Committee of Ministers to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies*. Kasutamise kuupäev: 25. June 2013. a., allikas Council of Europe: Committee of Ministers: https://wcd.coe.int/ViewDoc.jsp?Ref=Decl(12.06.2013)&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383

European Commission. (25. January 2012. a.). Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation).

Facebook. (31. March 2013. a.). *Newsroom*. Kasutamise kuupäev: 25. June 2013. a., allikas Facebook: http://newsroom.fb.com/Key-Facts

Fuchs, C. (2008). *Internet and Society: Social Theory in the Information Age.* New York: Routledge.

Gerstein, R. (1984). Intimacy and privacy. rmt: F. Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (lk 265-271). Cambridge: Cambridge University Press.

Greenwald, G. (9. June 2013. a.). *NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things' – video*. Kasutamise kuupäev: 10. June 2013. a., allikas The Guardian: http://www.guardian.co.uk/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

Group, M. M. (30. June 2012. a.). *Internet Usage Statistics: The internet Big Picture*. Kasutamise kuupäev: 25. June 2013. a., allikas Intenret World Stats: http://www.internetworldstats.com/stats.htm

Intellectual Property Watch. (9. July 2009. a.). *Hadopi2 passes French Senate*. Kasutamise kuupäev: 25. June 2013. a., allikas International Intellectual Property Policy: http://www.ip-watch.org/2009/07/09/hadopi-2-passes-french-senate/

Joseph, S. (2012). Social media, political change, and human rights. *Boston College International and Comparative Law Review, 35*(1), 145-188.

Laugen, L. (28. March 2013. a.). *Inimõiguste kohus: Eesti riik peab pronksiööl kinni peetutele hüvitist maksma*. Kasutamise kuupäev: 25. June 2013. a., allikas Delfi : http://www.delfi.ee/news/paevauudised/eesti/inimoiguste-kohus-eesti-riik-peab-pronksiool-kinni-peetutele-huvitist-maksma.d?id=65891912

Lucchi, N. (2010). Regulation and Control of Communication: The French Online Copyright Infringement Law (HADOPI). *Max Planck Institute for Intellectual Property and Competition Law Research Paper No. 11-07*.

Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age.* Princeton: Princeton University Press.

Moohr, G. S. (2003). The crime of copyright infringement: an inquiry based on morality, harm, and criminal theory. *Boston University Law Review, 83*(4), 731-783.

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics, 38*(8).

Moreham, N. (2006). Privacy in public places. *The Cambridge Law Journal, 65*(3), 606-635.

Moreham, N. (2008). The right to respect for private life in the European Convention on Human Rights: a re-examination. (J. Cooper, & A. McColgan, Toim-d) *European Human Rights Law Review, 13*(1), 44-79.

Pessach, G. (2007). An international-comparative perspective on peer-to-peer file-sharing and third party liability in copyright law: framing the past, present and the next genreations´ questions. *Vanderbilt Journal of Transnational Law, 40*(1), 87-133.

Ramón-Jerónimo, M. A., Peral-Pera, B., & Arenas-Gaitán, J. (2013). Elderly persons and internet use. *Social Science Computer Review, 31*(4), 389-403.

Randver, K. (2005). *Infoühiskonna digitaalne lõhe: selle põhjused ja mõju sotsiaalsele kaasatusele vanemas eas*. Kasutamise kuupäev: 25. June 2013. a., allikas Siseministeerium: https://www.siseministeerium.ee/public/Infouhiskonna_digitaalne_lohe..pdf

Recording Industry Association of America. (2013). *Piracy Online: Scope of the Problem*. Kasutamise kuupäev: 25. June 2013. a., allikas RIAA Web site: http://www.riaa.com/physicalpiracy.php?content_selector=piracy-online-scope-of-the-problem

Schmidt, E., & Manyika, J. (2011). Eric Schmidt on business culture, technology and social issues. *Internet Matters: Essays in Digital Transformation*, 200-206. McKinsey Global Institute.

Schoeman, F. (1984). Privacy: philosophical dimensions of the literature. rmt: F. Schoeman, *Philosophical Dimensions of Privacy: An Anthology* (lk 1-33). Cambridge: Cambridge University Press.

Scmidt, E., & Friedman, T. (23. May 2007. a.). *Eric Schmidt at the Personal Democracy Forum*. Kasutamise kuupäev: 25. June 2013. a., allikas Youtube: http://www.youtube.com/watch?v=ut3yjR7HNLU

Shahid, O. (25. October 2012. a.). *Immortal Technique: 'I'm seen as a threat to the status quo of hip-hop'*. Kasutamise kuupäev: 25. June 2013. a., allikas The Guardian : http://www.guardian.co.uk/music/2012/oct/25/immortal-technique-hip-hop-status-quo

Shane, S., & Somaiya, R. (16. June 2013. a.). *New Leak Indicates Britain and U.S. Tracked Diplomats.* Kasutamise kuupäev: 25. June 2013. a., allikas The New York Times: http://www.nytimes.com/2013/06/17/world/europe/new-leak-indicates-us-and-britain-eavesdropped-at-09-world-conferences.html?_r=0

Solove, D. (2008). *Understanding Privacy.* London: Harvard University Press.

Torremans, P. (2004). *Copyright and Human Rights: Freedom of Expression, Intellectual Property, Privacy.* London: Kluwer Law International.

World Economic Forum. (2013). Norms and Values in Digital Media: Shaping Solutions for a New Era. *Industry Agenda*.

World Intellectual Property Review. (24. January 2013. a.). *Hadopi Strikes at the Heart of Online Piracy*. Kasutamise kuupäev: 25. June 2013. a., allikas World Intellectual Property Review Web Site: http://www.worldipreview.com/news/hadopi-strikes-at-the-heart-of-online-piracy

## TABLE OF CASES

*BMG Canada Inc. v. John Doe*, 2004 FC 488, [2004] 3 FCR 241.

*BMG Canada Inc. v. John Doe*, 2005 FCA 193, [2005] 4 RCF 81.

*CCH Canadian Limited v. Law Society of Upper Canada*, [2004] 1 SCR 339,[1] 2004 SCC 13.

*Chapman v. the United Kingdom*, no. 27238/95, 8 January 2001, 33EHRR 18.

*Delfi As v. Estonia*, no. 64569/09, 11 February 2011 (pending).

*Dudgeon v. the United Kingdom*, no. 7525/76, 22 October 1981, 4 EHRR 149.

*Gaskin v. the United Kingdom*, no. 10454/83, 7 July 1989, 12 EHRR 36.

*Hatton v. the United Kingdom*, no. 36022/97, 8 July 2006, 37 EHRR 28.

*I v. the United Kingdom*, no. 25680/94, 11 July 2002, 36 EHRR 53.

*Korobov and Others v. Estonia*, no. 10195/08, 28 March 2013, ECtHR.

*Peck v. the United Kingdom*, no. 44647/98, 28 January 2003, 36 EHRR 719.

*P.G. and J.H.* v. the *United Kingdom*, no. 44787/98, 25 September 2009, ECHR 2001-IX.

*Rotaru v. Romania*, no. 28341/95, 4 May 2000, 8 BHRC 449, ECtHR.

*Segerstedt-Wiberg v. Sweden*, no. 62332/00, 6 June 2006, 44EHRR 4.

*Snyder v. Millersville Univ.*, No. 07-1660, 2008 U.S. Dist. LEXIS 97943.

*Van Kuck v. Germany*, no. 35968/97, 12 June 2003, 37 EHRR 51.

## LEGISLATION CITED

Canadian Copyright Act 1921.

Copyright Act 1709 (UK).

Criminal Justice and Public Order Act 1994 (UK).

Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society, 22 May 2001.

Directive 2004/48/EC of the European Parliament and of the Council, 29 April 2004, on the enforcement of intellectual property rights.

European Convention on Human Rights 1950.

French Hadopi law 2009.

French Intellectual Property Code, 1 July 1992.

Telecommunications Act 1984 and the Data Protection Act 1984.

Universal Declaration of Human Rights 1948.