UNIVERSITÀ DEGLI STUDI DI TRENTO
DIPARTIMENTO DI SCIENZE GIURIDICHE
Scuola di Dottorato in Studi Giuridici
Comparati ed Europei

Scuola di Dottorato in Studi Giuridici Comparati ed Europei

XXIV ciclo

Tesi di dottorato

Balancing Conflicting Rights In the Digital Age

The Case of Information Privacy vs. Copyright Enforcement Against File Sharing

Relatore
Prof. Roberto Caso

Dottoranda
Federica Giovanella

Anno Accademico 2010 – 2011

Curriculum di Diritto privato, privato comparato e commerciale

XXIV ciclo

Commissione esaminatrice:

Prof. Giovanni Sartor, Università degli studi di Bologna
Prof. Giorgio Resta Università degli studi di Bari
Dott. Massimiliano Granieri, Università degli studi di Foggia

Esame finale: 12 aprile 2012

TABLE OF CONTENTS

Abstract

The research, employing a comparative and multidisciplinary approach, aims at understanding the conflict between information privacy and copyright enforcement in the digital era. Throughout the whole study attention will be paid to the effect that technology has on these rights. The systems under scrutiny will be the European one (with particular regard to Italy) and the North American ones (US and Canada).

The starting point of this analysis are a number of selected lawsuits in which copyright holders have tried to enforce their rights against Internet users suspected of illegal peer-to-peer downloading. In so doing, copyright enforcement collided with users' information privacy. In analyzing the way in which these decisions were taken, I shall try to understand how technology affects society. Many studies have demonstrated the interaction between technology and society. Copyright and information privacy laws are themselves a product of technology and innovation.

The idea behind my analysis is that technology not only affects society, but that it also affects lawmakers, and even judges (who, directly or indirectly, are lawmakers as well). Indeed, judges do not live a secluded life, but operate within a society. Therefore, it is at least plausible, if not necessary, that their decisions reflect the values of that society. In other words, technology influences society, which, in turn, affects judicial opinion.

To assess if my statement is sound, I shall consider the perception of copyright, limited to file-sharing activities, in the three normative systems. The same analysis will be undertaken with regard to information privacy. As will be seen, unsurprisingly, technology has affected in many ways the substance of both privacy and copyright norms. But technology has also affected people's lives, people's way of behaving, and, in the end, people's minds. This has led to a different perception of the need to protect the aforementioned rights, even if in opposite directions. Privacy concerns have been increasing, while copyright is more and more seen as something "negative", for a variety of reasons. Given this, a plausible answer to my main line of inquiry is that courts' decisions reflect this common sense position of prioritizing privacy over copyright.

In particular, I shall examine the literature related to the way courts judge and if and how they can be influenced by the society and culture in which they operate. Importance will be given to the way that this influence could enter into judicial reasoning. If it is true that technology changes society, which in turn affects the judicial mind, then technology enters into this contextual backdrop for adjudication. Therefore, the question I would like to answer is the following: could this be a reason why, despite similar legal frameworks, the outcomes of lawsuits are quite different among the considered legal systems? This would be the goal of my research, conscious of the fact that anyway my answer would be just one of the many possible explanations.

Chapter 1
What This Work Would Like To Be

"When the law is asked to solve a problem created by a new technology, it is hard for the law to "get it right" unless decisionmakers understand not just the technology, but the social and cultural uses of the technology as well"
L. BARNETT LIDSKY (2009)

Law and technology have influenced each other for ages: law has enabled the development and application of new techniques; technology has helped law in reaching its goals. Technology has also deeply affected the way people think and behave, modifying the entire society. Therefore also individuals' economic behavior has changed.

Despite the fact one would immediately think about the great impact of digital technologies and the Internet, important changes took place also with older innovations, going back to the invention of movable type[1]. History shows that this invention, as long as many other fundamental innovations, has imposed important changes in the diffusion and application of law. One could draw the same conclusion regarding digital technologies, including the Internet, in what it is called "digital era"[2].

Furthermore, many studies have demonstrated the interaction between technology and society. Copyright and information privacy laws are themselves a product of technology and innovation. History shows that before the invention of movable typefaces copyright was in fact a marginal problem[3]. Moreover, when Warren and Brandeis wrote their seminal article, they were concerned with the invention of a portable camera that could threaten people's private lives, whose

[1] G. PASCUZZI, *Il diritto dell'era digitale*, Bologna, 2010, 11 ff. argues that the first technology which affected irreparably the use of law was the introduction of writing.
[2] PASCUZZI, *Il diritto dell'era digitale*, cit., 14 ff. Prof. Pascuzzi's expression "digital era" refers to a time when representation, elaboration and communication of information have changed due to digital technologies. In particular: before the intervention of those technologies, we could imagine original works only on material supports; now these works can be represented with numbers, through the binary code. As a consequence, the elaboration is quick and easier. Finally, thanks to information and communication technologies, data can be transferred to everywhere in few seconds.
[3] This invention is actually the spark from which copyright was born; see U. IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico*, Roma, 2010, *passim*.

pictures could be put in tabloids[4]. Throughout the twentieth century, digital technologies shifted the attention from the so-called "right to be let alone" to the "informational aspect" of people's lives. Personal data protection has then always been thought as a part of privacy or, at least, as an instrument to protect people's privacy.

Copyright and privacy are also two of the most discussed topics in the current academic scholarships and it has been so for decades now. They have been analyzed deep and wide by scholars of different disciplines, being law only one of the lenses through which these two important issues can be examined. In particular, the advent of the so called digital technologies increased the debate with regard to those places where the two topics collide[5].

In the last three decades an increasing number of cases have pertained to the enforcement of copyright. Some of these decisions have drawn the attention not only of scholars, but also of the media. More recently, this type of disputes caused a great stir through the Internet, since end users are often part of the play.

The starting point of this work is represented by some lawsuits in which the contrast between copyright and data protection emerges patently. I selected these cases because they are the expression, in each of the country of reference, of the conflict analyzed in this work. In these lawsuits, copyright holders have tried to

[4] I am referring to S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, 4 Harvard Law Review 193 (1890). See *infra* for some details on this article. The article can be found at http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. [All the websited cited in this work were last visited on March 10, 2012].

[5] Just to give some examples of the attention paid by scholars to the conflict between copyright and privacy see the dossier of Institute for Information Law: *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems*, Amsterdam, 1998 available at http://www.ivir.nl/publications/koelman/privreportdef.pdf. See also the important contributions of J. COHEN, *DRM and Privacy*, 18 Berkeley Tech. L.J. 575 (2003); A. CAMERON, *Digital Rights Management: Where Copyright and Privacy Collide*, 2 Canadian Privacy Law R. 14, (2004); S.K. KATYAL, *Privacy v. Piracy*, 7 Yale J. Law & Tech. 222 (2004); M.A. WILKINSON, *Battleground between new and old orders: control conflicts between copyright and personal data protection*, in Y. GENDREAU (ed.), *Emerging Intellectual Property Paradigm: Perspectives from Canada*, Cheltenham, 2008, 252 ff.. For the European scenario: R. LATTANZI, *Protezione dei dati personali e diritti di proprietà intellettuale: alla ricerca di un difficile equilibrio*, in *Jus*, n. 1-2/2005, 233 ff; A. PALMIERI, *DRM e disciplina europea della protezione dei dati personali*, in R. CASO (ed.), Digital rights management*: problemi teorici e prospettive applicative*, Trento, 2008, 197, available at http://eprints.biblio.unitn.it/archive/00001336/. See also the entire volume 4, issue 2 of the John Marshall Review of Intellectual Property Law (4 J. Marshall Rev. Intell. Prop. L. 212 ff. (2005), available at http://www.jmripl.com.php5-10.dfw1-2.websitetestlink.com/issues/archives/4/2) where prominent scholars discuss the relationship between copyright and privacy as seen through different lenses, such us the privacy lens, the technology lens, the copyright lens, and so on. Other contributions to this topic will be cited throughout the work.

enforce their rights against Internet users suspected of illegal peer-to-peer downloading. To put it simply, peer-to-peer is a way for users to exchange files through the Internet[6]. Among the most frequently exchanged files are songs and movies, which usually circulate without the permission of the copyright holder.

To enforce their rights, copyright holders need to find out the real identities hidden behind computers. In fact, end users can normally be identified only through pseudonymous or Internet Protocol (IP) addresses[7]. These numbers are usually found by specialized service companies which, through different methods, can crawl in the Net and discover the IP addresses. Once copyright owners have these addresses, they still need the collaboration of Internet Service Providers (ISPs)[8] to obtain users' real identities. Only ISPs can indeed match IP addresses with their customers' information. Some ISPs have denied their collaboration, forcing copyright holders to ask courts to decide whether the providers should cooperate or not. These are the lawsuits which stay at the core of my work.

In these processes, courts have reacted in different ways. Nonetheless, independently from their final decision, the majority of them have touched the issue of users' information privacy and/or anonymity protection. Even if courts did not concentrate their main argumentations on privacy or anonymity, they nevertheless have always at least mentioned the question. This raises a conflict between the need of copyright holders to enforce their right and the right of users to their anonymity or information privacy. In particular, this conflict and the way courts have tried to solve is the core of this work.

As it will be shown in the following chapters, judges are well aware of the difficulties of balancing the mentioned rights. In my view, a correct resolution of this conflict would require a precise scheme, in which both rights can be weighed in order to understand which one is the most important in every single case.

[6] I will give a better account of this phenomenon and of its development in the next chapter; for a deep explanation see for example R. STEINMETZ, K. WEHRLE, *Peer-to-peer systems and applications*, Berlin - New York, 2005, 10 ff.

[7] An IP number is "a unique number that identifies the precise location of a particular node on the Internet. The address is a 32-bit number usually written in dotted decimal format, i.e. in the form '123.33.22.32', and it is used by the TCP/IP protocol", see *Entry: Internet Address*, S.M.H. COLLIN, *Dictionary of Computing*, London, 2004. IP addresses can be static or dynamic, for more details see *infra*.

[8] ISP is "a company that provides one of the permanent links that make up the Internet and sells connections to private users and companies to allow them to access the Internet", *Entry: ISP*, COLLIN, *Dictionary of Computing*, cit.

Nonetheless, not in every of the considered systems there is such a scheme and, in addition, where a scheme exists, it is not always clear how the two rights are actually weighed. Indeed, it will be illustrated how in every case judges have a more or less high degree of discretion. If, on the one hand, every judicial decision normally implies discretion, on the other hand this can lead to situations where judges do not apply – strictly speaking – law. This is what my thesis is based on.

This work goes beyond the mere aspect related to judicial decisions in which law is not clear and fundamental values – such as information privacy or anonymity – are put under pressure. In particular, my hypothesis is that, in the absence of a precise "value scale" dictating how to manage different rights and weigh them one against the other, judges apply rules according to the social perception of the conflicting values. In doing so, they act not only as law makers, but also as policy makers[9].

As it has been often claimed and demonstrated, privacy is a cultural concept. Different peoples perceive and live privacy in different ways[10]. This is somehow mirrored by the different legal approaches taken by the systems here considered. At the same time it is reflected into judicial decisions.

I think a similar argument could be advanced in relation to copyright. More precisely, it could be put forward with regard to the influence that technology has been having on copyright and the reactions taken by different systems. Governments are supposed to take decisions in order to modify legislation so that it can answer, or perhaps anticipate, technological developments. When governments do not take action with regard to these developments, judges act as law makers and create rules where they need to be created.

To assess if my statement is sound, I shall consider the perception of copyright, limited to file-sharing activities, in the three normative systems. The same

[9] It can be understood that my research will be primarily a descriptive one. Nevertheless, a prescriptive approach could sometimes emerge, since in my opinion description and prescription are not always easily distinguishable and divisible.

[10] Anthropologists have studied privacy of many different peoples and nations, concluding that privacy is universally present in different societies, even if it shows itself in diverse manners. See, among others, J.M. ROBERTS, T. GREGOR, *Privacy: A cultural view*, in J.R. PENNOCK, J.W. CHAPMAN (eds.), *Privacy*, New York, 1971, 199. In the same book see also the contribution of H.J. SPIRO, *Privacy in comparative perspective*, at 121. See also I. ALTMAN, *Privacy Regulation: Culturally Universal or Culturally Specific?*, 33 Journal of Social Issues 66 (1977). For a more recent writing cf. J.Q. WHITMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 Yale Law Journal 1153 (2004).

analysis will be undertaken with regard to information privacy. As it will be seen, unsurprisingly, technology has affected in many ways the substance of both privacy and copyright norms. But technology has also affected people's lives, people's way of behaving, and, in the end, people's minds. This has led to a different perception of the need to protect the aforementioned rights, even if in opposite directions. Privacy concerns have been increasing, while copyright is more and more seen as something "negative", for a variety of reasons. Given this, a plausible answer to my main line of inquiry is that courts' decisions reflect this common sense position of prioritizing privacy over copyright.

For the sake of a better understanding of my work, I shall clarify the meaning of the word "privacy" as used in this research. Indeed, unlike copyright, which is a legal concept, "[t]he term "privacy" is an umbrella term, referring to a wide and disparate group of related things. The use of such a broad term is helpful in some contexts yet quite unhelpful in others"[11].

For decades, scholars have been trying to give a precise definition of "privacy"[12]. It has been effectively claimed that "[p]erhaps privacy is so hopelessly diffuse as to be virtually indistinguishable from the related concepts of liberty, autonomy and freedom"[13]. The number of different attempts to delineate privacy is so high that I will not even try to recap them[14]. Rather, I would prefer setting immediately a "given" definition, which will be applied throughout the rest of the work. Actually, I will join someone else's definition of privacy "as the ability of an individual to exercise control over how his/her personal information is collected, used or disclosed by third parties"[15]. This definition is very close to the one regarding the "protection of personal data", which is at the core of this research. Indeed, the collection and use of personal information can have a great impact on an individual's privacy. Probably due to that, the two concepts are often overlapped. I somehow embrace this overlap, which is often also embraced by laws and statutes, as well as

[11] D.J. SOLOVE, *A Taxonomy of Privacy*, 154 U. Pennsylvania Law Review 477 (2006), 485.
[12] See the ironic words of H. NISSENBAUM, *Privacy in Context. Technology, Policy, and the Intergity of Social Life*, Standford, 2010, 2-3.
[13] C.J. BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, Ithaca (NY), 1992, 26.
[14] For a summary and brief explanation of the "leading definitions" of privacy, see C.H.H. MCNAIRN, A.K. SCOTT, *Privacy Law in Canada*, Markham, 2001, 4 ff.
[15] M.S. HAYES, *The Impact of Privacy on Intellectual Property in Canada*, 20 Intellectual Property Journal 67 (2006), 68.

by judges. This is consistent also with the appellation "information privacy", that can be seen as a crasis of the two concepts: physical privacy and personal data protection.

In this sense another interesting definition which could be applied in this work is the one offered from the Australian Privacy Commissioner: "[i]nformation privacy concerns the handling of 'personal information', that is, information about a particular person or information that can be used to identify a particular person"[16]. The definition is also very close to Alan Westin's one, for whom information privacy is "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others"[17]. The manner personal information is diffused can represent individuals' way of being, with relation to personal identity[18].

Given these premises, my aim is trying to demonstrate that the decisions taken in the previously mentioned lawsuits are in some way influenced by the perception of privacy and the conception of copyright in the considered systems. I am conscious that my attempt, even if feasible, would give only one of the possible explanations for these decisions. In fact, many different variables can play a role. To give an example, lobbies can have a great impact not only on Congress, but also on judges. This makes it difficult to understand which variables really affect judicial decisions and to what extent.

In the enforcement of copyright there has always been a duty to balance (at least) two conflicting interests: the right(s) of the owner and the right(s) of the user[19]. This is at the very end the same conflict between the copyright owner's right to enforce her copyright and the end user's right to privacy. We can therefore say that behind the conflict between copyright and data protection lays such bigger conflict. This is mainly the reason why, before analyzing the mentioned cases related to peer-

[16] "What Is Information Privacy And Why Do We Need To Protect It?" in *Information Privacy In Australia: A National Scheme For Fair Information Practices In The Private Sector*, Australian Privacy Commissioner, August 1997, online at: http://austlii.edu.au/itlaw/national_scheme/national-PART.html

[17] Cf. A.F. WESTIN, *Privacy and Freedom*, New York, 1967, 7. On these definitions I will base my work. Therefore, unless otherwise specified, I will use the term "privacy" as a synonym for information privacy, which is actually the real target of my research.

[18] G. BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Milano, 1997, 95.

[19] To give an example, the so called *Sony Betamax* case was, in the end, a contrast between the copyright of the plaintiffs' and the users' right to use the Sony Betamax in the way they liked; for an explanation of this case see *infra* par. 2.3.1.

to-peer, I shall first explain some older cases, which do not necessarily cope with data protection, but that indicate the persistent question of the enforcement of copyright in the last thirty years. These cases demonstrate that the problem is constant and worldwide.

After giving a picture of the current situation, my analysis will outline the legal framework of privacy and data protection in each of the systems. The same will then be done with copyright and illegal download. I will then pay attention to the sociological frame that prominent scholars have proposed for both the concepts of privacy and copyright.

In the final part I will try to outline some conclusions, with the aim of understanding the solution for the conflict between these two rights. In particular, my idea is that, where law is not clear, judges interpret it according to the perceptions and conceptions of the society in which they live. In this way they are policy makers and, in my view, this is what has happened at least in some of the considered lawsuits.

Before approaching the next parts of this work, I want to beware the reader of some limits of this research. As one can have already understood, this work takes into account only the enforcement of copyright, even though other intellectual property rights could face the same problems considered here. At the same time the research is narrowed to the violation of copyright committed through peer-to-peer systems. Moreover, privacy is not the only right which can be in contrast with copyright, since also freedom of speech or property can be. Once again: it can be possible that situations like those investigated here exist also for infringement perpetrated with other means and to other rights. The idea behind this work is to draw out from some practical cases one or more general rules, applicable to different scenarios.

The work presents first the three systems. For every of them the legal framework of privacy and data protection is considered, as well as the regulation of copyright and peer-to-peer. The last chapter tries to sketch some descriptive conclusions in the mentioned direction, conscious that my attempt will be anyway be partial and deficient.

Chapter 2
The American System

2.1 The legal framework for file sharing

Unlike other important legal systems, the US Constitution contains the "legal source" of intellectual property protection. More precisely, Section 8, Article 1 of the US Constitution famously states: "The Congress shall have the power […] [t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries". This Section provides not only the basis for the power of Congress to legislate in the field of intellectual property, but it defines also the rationale that should sustain such action. In what might be considered a typically utilitarian approach[1], Section 8 tries to balance the encouragement of intellectual creativity with the need to keep intellectual products circulating freely in society.

As in Canada, in the US there is no longer a common law of copyright[2], which is superceded by and regulated only through the *Copyright Act*. The Act, which represents Title 17 of the U.S. Code (U.S.C.), has been frequently amended and has been the subject of important judicial interpretations. The current *Copyright Act* was introduced in 1976[3], after decades of work, to replace the previous Act[4], considered too basic for the scope of modern American society. The Act expanded both the scope and the duration of copyright protection, introducing also a preemption provision in favor of federal institutions. Therefore, the Act expressly states that "no person is entitled to any such right or equivalent right in any such work under the common law or statutes of any State"[5].

---

[1] R.P. MERGES, P.S. MENELL, M.A. LEMLEY, *Intellectual Property in the New Technological Age*, New York, 2010, 11 ff.

[2] This was made clear already in *Wheaton v. Peters*, 33 U.S. (Pet. 8) 591 (1834). Nevertheless, prior to the enactment of 1976 *Copyright Act*, a common law or state law copyright was recognized in unpublished works. S.W. HALPERN, C.A. NARD, K.L. PORT, *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, Alphen aan den Rijn, 2011, 2.

[3] Enacted on October 19, 1976, as Pub. L. No. 94-553, into effect from the beginning of 1978.

[4] The previous Copyright Act was enacted on March 4, 1909, as Pub. L. No. 60-349.

[5] 17 U.S.C. § 301(a). According to this section, "no person is entitled to any such right or equivalent right in any such work under the common law or statutes of any State".

The protected categories are listed in section 102, which comprise, among others, "musical works, including any accompanying words" and "sound recordings". The listed categories are not meant to be exclusive, as they function as administrative categories for the registration of copyrighted works[6]. Despite the possibility of registration, copyright does actually exist in all original creative expressions, as long as they are "fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device"[7].

Section 101 of the Copyright Act provides with a number of definitions, such as "sound recordings", which "are works that result from the fixation of a series of musical, spoken, or other sounds, but not including the sounds accompanying a motion picture or other audiovisual work, regardless of the nature of the material objects, such as disks, tapes, or other phonorecords, in which they are embodied". Sound recordings were not covered by copyright until 1972, when the *Sound Recording Amendment* provided for the protection in the performance of a work independent of the copyright in the work being performed[8]. Curiously, this amendment was introduced "to provide for the creation of a limited copyright in sound recordings for the purpose of protecting against unauthorized duplication and *piracy* of sound recording, and for other purposes"[9].

Thanks to section 114, the owner of a sound recording copyright has the exclusive right to:

- duplicate her work in the form of phonorecords or copies that directly or indirectly recapture the actual sounds fixed in the recording;
- create derivative works which the sound fixed in the sound recording are rearranged, remixed, or otherwise altered in sequence or quality;
- to publicly distribute copies of the sound recording;

[6] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 5.
[7] 17 U.S.C. § 102(a).
[8] Act of October 15, 1971, Pub. L. No. 92-140 modifying the *Copyright Act* of 1909. As it will be illustrated in the next chapter, neighbouring rights obtained protection only relatively recently in Canada as well.
[9] Emphasis added. The Act was consistent with *Geneva Convention for the Protection of Producers of Phonograms against Unauthorized Duplication of Their Phonograms*, that has entered into force in US in 1974.

- and to publicly perform the recording "by means of any digital audio transmission".

Except from this last right, the owner of a sound recording does not have any public performance right on the recording itself. US lawmakers are, in any event, undertaking "continuing legislative efforts" to broaden the performance right in sound recordings[10]. Prior to 1978 some requirements were needed for an author to acquire copyright on a work. In particular, the work had to be registered, deposited and accompanied with appropriate notice in order to become protected by the federal law. If the notice was not there, protection would have been lost and the work would have fallen into the public domain. As said, with the current *Copyright Act*, common law copyright was eliminated and also the distinction between published and unpublished works, together with the mentioned formalities[11]. Nowadays, what counts is that the work has been fixed in any tangible medium of expression, as required by section 102. The work should be perceived, reproduced or otherwise communicated from this medium, with or without the aid of a machine. Paragraph 101 defines as "fixed in a tangible medium of expression" a work which is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration". As is also the case in Canada, there remains the possibility to register a work and make a deposit of a copy of the same. In particular, three formalities currently exist: notice, deposit and registration[12]. Despite under the 1976 Act formalities are not a condition affecting the existence of the right, they remain important for some consequences they bring[13]. Deposit and registration affect the ability to enforce copyright and to obtain certain remedies. Registration is, for example, a pre-requisite for an action for infringement of a "United States work"[14]. In an action for infringement, registration helps with some procedural and remedial issues, which are not available for unregistered works. For example, if the work was registered within five years after

[10] Cf. HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 38.
[11] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 40 ff. This was made also to comply with the *Berne Convention for the Protection of Literary and Artistic Works*, September 9, 1886.
[12] On formalities see M. LAFRANCE, *Copyright Law in a Nutshell*, St Paul, 2008, 95-114.
[13] Cf. HALPERN, *Copyright Law. Protection of Original Expression*, cit., 430 ff.
[14] 17 U.S.C. § 411. This requisite is limited to US works in order to not affect foreign authors, as required by the *Berne Convention*. Cf. LAFRANCE, *Copyright Law in a Nutshell*, cit., 287 ff.

its first publication, the certificate of registration is a *prima facie* evidence of the validity of the copyright, as well as of the fact stated in the certificate[15]. Registration also has an impact on the damages recoverable by the plaintiff[16].

Going back to the protection afforded by the 1976 *Copyright Act*, paragraph 106 provides a closed list of rights, which is complete and exhaustive[17]. The copyright holder possesses the right to do and to authorize any of these following acts:

1. to reproduce the copyrighted work in copies or phonorecords;
2. to prepare derivative works based upon the copyrighted work;
3. to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
4. in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;
5. in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and
6. in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

As it can be understood, the first three rights are applicable to all categories of copyrightable works, while the other three apply only to the works they mention. For our analysis of the file-sharing context, only some of these rights are obviously to be taken into account and will therefore be analyzed here.

The first is the right to reproduce, meant as the basic copyright protection, comprising also the making of "phonorecords"[18]. There is a "tangibility requirement"

[15] 17 U.S.C. § 410(c). Furthermore, certain formalities continue to have a key role in determining the copyright status of works that were first published within February, 1989, cf. LAFRANCE, *Copyright Law in a Nutshell*, cit., 95.

[16] Cf. 17 U.S.C. § 412: only if registration precedes the act of infringement or infringement begun after first publication, even if before registration, the plaintiff can recover statutory damages and attorney fees.

[17] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 70.

[18] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 70; LAFRANCE, *Copyright Law in a Nutshell*, cit.,159.

that applies both to copies and to phonorecords[19]. As previously mentioned, the *Act* itself defines "copies" as material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. "Copies" are the material objects, other than a phonorecord, in which the work is first fixed. The *Act* further recognizes "phonorecords" as "material objects in which sounds, other than those accompanying a motion picture or other audiovisual work, are fixed by any method now known or later developed, and from which the sounds can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device"[20]. The term "phonorecords" includes the material object in which the sounds are first fixed. Hence, the Act does not take into account the nature of the copying device, or the medium or the methodology used[21]. The difference between the two is that while a phonorecord is the tangible fixation of sounds, a copy is any tangible fixation other than a phonorecord[22]. Typically, the duplication of an mp3 file on a computer or other electronic recording devices would be considered to be a copy. Copying also occurs when files are uploaded from a computer to a server and when they are shared among computers, adding the material to the hard disk of the recipient's PC while retaining a copy in the sender's computer hard disk[23].

The reproduction right is independent from the public distribution right: reproduction right is therefore breached as soon as a copy is made, regardless of whether that copy is distributed or not[24].

The *Act* specifically provides an exemption for the non-commercial use of a consumer who makes digital or analog copies of musical recordings[25]. The source of

[19] LAFRANCE, *Copyright Law in a Nutshell*, cit., 160.
[20] 17 U.S.C. § 101.
[21] Some types of reproduction are simply called in a different way and treated accordingly, see HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 71.
[22] Therefore, "an mp3 file of a sound recording is a phonorecord, while a DVD, or any other tangible embodiment of an audiovisual work, is a copy", cf. LAFRANCE, *Copyright Law in a Nutshell*, cit., 160.
[23] It remains unclear whether the temporary copy on a random access memory (RAM) of a computer could be an infringement, since § 101 asks "for a period of more than transitory duration". The majority of courts have held that temporary storage on RAM *is* a fixation; nevertheless, one court suggested that there would not be a fixation when it is automatic and transitory, as in the case of transmission through the facilities of an ISP (see *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F3d 544 (4th Cir. 2004) at 551); cf. LAFRANCE, *Copyright Law in a Nutshell*, cit., 161-162.
[24] LAFRANCE, *Copyright Law in a Nutshell*, cit., 163.

this norm was the introduction of digital audio taping technology (DAT). This technology enabled the user to obtain on tape high fidelity copies, in a way close to the later CD system. The recording industry, which feared this digital recording, strongly protested against the importation of DAT. As a result, the *Audio Home Recording Act* (AHRA) added Chapter 10 – "*Digital Audio Recording Devices and Media*" to Title 17 of the U.S.C.[26] The provision intends to prevent the making of wholesale copying of a work. A royalty obligation is imposed on manufacturers or importers of equipment used for digital audio; these royalties are then distributed among recording companies, publishers and composers[27]. It was the first time that American government imposed "technological design constraints on the manufacture of copying recording media"[28]. With the improvements of technology, this provision got obsolete, so that courts held that a computer hard disk is not a "digital audio recording device", nor is an MP3 player. As a consequence the manufacturer of an MP3 player that records from a hard drive is not subject to the inhibitions and to the royalties of the mentioned chapter[29]. For the same reasons, the Ninth Circuit also claimed that the noncommercial downloading of copyrighted music from the Internet through a computer is not immunized by section 1008[30].

Mechanical copies of musical works can be made and distributed without the consent of the copyright owner, when a person pays a compulsory license for "making and distributing phonorecords" other than dramatic musical work[31]. This is possible only if the primary purpose of the copying is to distribute the phonorecords to the public for private use[32]. In 1995, through the *Digital Performance Right in*

---

[25] 17 U.S.C. § 1008. See § 1001 for definitions regarding this chapter of the *Copyright Act*.
[26] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 77. AHRA was of an Act of October 28, 1992, Pub. L. No. 102-563, 106 Stat. 4237.
[27] 17 U.S.C. § 1001 ff.
[28] MERGES ET AL., *Intellectual Property in the New Technological Age*, cit., 668. The system allowed users to make copies directly from a compact disc, but not from digital copies made using this technology. The aim was to limit "second-generation" copies.
[29] *RIAA v. Diamond Multimedia System, Inc.*, 180 F.3d 1072 (9th Cir. 1999), 1081. For a brief overview of the case, see below.
[30] *A&M Record Inc. v. Napster, Inc.*, 239 F.3d 1004 (2001), 1024. See *infra* for a summary of the decision.
[31] For an account of the actual functioning of the licenses, see HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 79-80.
[32] 17 U.S.C. § 115, which determines also the provisions, limitations, and procedure to acquire the compulsory license, as well as to determine the payment of royalties.

Sound Recordings Act[33], the license was extended to digital audio delivery of nondramatic musical work. This license covers only the "phonorecords" distribution and not any and all other kinds of reproduction of a copyrighted work[34].

As mentioned, copyright owners also hold the exclusive right "to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease or lending"[35]. This right recalls the old common law right of "first publication"[36], giving the creator of a work the possibility to decide if and when that work would be exposed to the public. It is worth noting that this right "is distinct from the other rights, so that permission, for example, to copy, or to perform a work, would not include permission to make public distribution of those copies"[37].

Despite the fact that the *Copyright Act* does not give a definition of "distribution", section 101 defines "publication" as the "distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending". The definition of "publication" includes also a mere "offer to distribute" copyrighted material for further distribution or public performance or public display. This led courts to conflicting decisions on whether a public distribution takes place when files are "made available" on the Internet, without proof of an actual copy or distribution of the material. Most courts have claimed that downloadable Internet transmissions are indeed a form of public distribution, given that people receiving a downloadable transmission can save a non-transitory copy. This raises the additional issue whether the distribution occurs when the recipient actually downloads the files or, rather, when the material is just made available[38]. Some amendments were recommended in order to include "transmission" as a "distribution" and also to define "publication" to include "transmission", so that the transmitter would be infringing these rights when she diffuses them. Congress did not welcome this proposal, even if some courts did. In fact, it has been held that

[33] An Act of November 1, 1995, Pub. L. No. 104-39, 109 Stat. 336. See 17 U.S.C. § 114 (d).
[34] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 79.
[35] 17 U.S.C. § 106 (3).
[36] S.W. HALPERN, *Copyright Law. Protection of Original Expression*, Durham, 2010, 252.
[37] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 83.
[38] LAFRANCE, *Copyright Law in a Nutshell*, cit., 173-177 *sic passim*.

Internet transmission of a sound recording is an act infringing "distribution right" on the sound recording and of the copyrighted music it contains[39]. There have also been different opinions, holding that a defendant cannot be considered liable for public distribution if no copy of the work is actually found on the defendant's system[40].
When considering musical works, one should remember that section 106(4) protects the right "to perform the copyrighted work publicly"[41]. The key elements of this definition are the words "perform" and "publicly". As usual, section 101 provides some definitions: "[t]o "perform" a work means to recite, render, play, dance, or act it, either directly or by means of any device or process or, in the case of a motion picture or other audiovisual work, to show its images in any sequence or to make the sounds accompanying it audible". Any act which makes a copyrighted work to be perceived by the viewer or the listener, or causes a work to be reproduced, is a performance[42]. Hence, performances can be done by a "human" performer (such a singer or an orchestra), as well as through a music player[43]. Moreover, the Act states that a separate performance occurs when there is a transmission or re-transmission of a performance of a copyrighted work[44].

The definition of publicly is once again offered by section 101. "To perform or display a work "publicly" means - (1) to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or (2) to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times". As can immediately be understood, "public" is related to the place where the performance is done. So, when a place is open to the public, such as a videocassette rental store

[39] *A&M Record Inc. v. Napster, Inc.*, cit., 1013 stating: "[w]e agree that plaintiffs have shown that Napster users infringe at least two of the copyright holders' exclusive rights: the rights of reproduction, § 106(1) and distribution, § 106(3)".
[40] *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007), 1162.
[41] It is essential to distinguish between the rights in a sound recording and those in a musical composition. Sound recordings enjoy a different kind of public performance right, under § 106(6), cf. LAFRANCE, *Copyright Law in a Nutshell*, cit., 177.
[42] MERGES ET AL., *Intellectual Property in the New Technological Age*, cit., 572.
[43] In this case, the performer would be the person who made the player play.
[44] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 91.

showing rented videocassettes in small rooms, the performance is considered public[45]. A performance could still be public even if it is made in a private place, but in front of a "substantial number" of people, depending also on the nature of the occasion and the relationship among the members of the audience[46].

According to section 101, "transmit" means to communicate a performance "by any device or process whereby images or sounds are received beyond the place from which they are sent". Transmission of a performance to the public is considered as such when recipients receive it simultaneously or sequentially, as in the case of a hotel showing a movie in individual rooms upon request of its guests[47]. Streaming audio or video transmissions on the Internet can be a performance when they can be received by members of the public, even if it is received by different people in different places and in different moments. Therefore, despite the fact that a streaming transmission cannot be considered a public distribution because it cannot be downloaded[48], it nevertheless is a public performance[49].

Despite, as mentioned above, the fact that the original version of the *Copyright Act* did not include performance rights as a part of the exclusive rights of the owner of copyright in a sound recording, the *Digital Performance Right in Sound Recording Act* introduced this neighbouring right "to perform the copyrighted work publicly by means of a digital audio transmission"[50]. This right applies only to sound recordings and to transmissions which are "in whole or in part in a digital or other non-analog format"[51]; therefore, for example, it would neither be applied to radio

[45] Cf. *Columbia Pictures Industries, Inc. v. Redd Home, Inc.*, 749 F.2d 154 (3d Cir. 1984), 158-159: "[t]he remaining question is whether these performances are public. Section 101 […] is written in the disjunctive, and thus two categories of places can satisfy the definition of "to perform a work publicly." The first category is self-evident; it is "a place open to the public." The second category, commonly referred to as a semi-public place, is determined by the size and composition of the audience. Clearly, if a place is public, the size and composition of the audience are irrelevant. However, if the place is not public, the size and composition of the audience will be determinative. […] We find it unnecessary to examine the second part of the statutory definition because we agree with the district court's conclusion that [it] was open to the public; […] "the showcasing operation is not distinguishable in any significant manner from the exhibition of films at a conventional movie theater."

[46] LAFRANCE, *Copyright Law in a Nutshell*, cit,, 179-180; HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 92.

[47] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 91-92.

[48] Actually there are "video streaming recording" softwares which allow this action.

[49] LAFRANCE, *Copyright Law in a Nutshell*, cit., 182.

[50] 17 U.S.C. § 106(6).

[51] See the definition of "digital transmission" in § 101 of the *Copyright Act*.

broadcast stations nor to prerecorded music played in restaurant, since it is applied only to "transmissions"[52]. The *Digital Millennium Copyright Act* (DMCA)[53] deeply modified this section of the *Copyright Act* in order to expand its scope: it now comprises Internet performances and contains a licensing scheme, as well as measures aimed at stopping so-called piracy[54].

All the rights recognized by the *Copyright Act* are limited in time. The mentioned Section 8 of the Constitution requires such a limitation, which has been therefore specified by the Congress in the legislation. The Act of 1976 significantly changed the previous scheme, which was based on a dual-term system with fixed terms of years[55]. The term introduced in 1976 was 50 years after the death of the author[56], but was extended by other 20 years through the *Copyright Term Extension Act* of 1998[57].

As stated above, major amendments have been introduced and consistently modified the *Copyright Act* original provisions. Indeed, as it has been noticed, "[d]espite the relative simplicity of th[e] aim [of Section 8, Clause 8 of the Constitution], Congress has recognized a need continually to realign copyright law in the wake of historical changes in the technology, politics, culture, and economics of information production"[58].

---

[52] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 107.
[53] An Act of October 28, 1998, Pub. L. 105-304, 112 Stat. 2860.
[54] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 107-108; LAFRANCE, *Copyright Law in a Nutshell*, cit., 188.
[55] For an account of the previous system, see HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 136-139.
[56] The starting point for the run of the term can vary depending on the type of work, see HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 141 ff; LAFRANCE, *Copyright Law in a Nutshell*, cit., 115 ff. See also HALPERN, *Copyright Law. Protection of Original Expression*, cit., 434 ff. and the table reported in MERGES AT AL., 509.
[57] The Act is more commonly known as "*Sonny Bono Act*" from the name of the singer (then) politician Member of the Parliament who greatly sponsored the extension of copyright terms. The Act is also called, perhaps pejoratively, "*The Mickey Mouse Protection Act*" due to the well-known lobbing efforts of the Walt Disney Company. This amendment to the Copyright Act was harshly criticized, since it stopped the advancement of the US public domain. In particular, the constitutionality of this extension with respect to Section 8 was challenged by some publishers and librarians. The case was heard by the Supreme Court in *Eldred v. Ashcroft*, 537 U.S. 186 (2003), which held: "we find that the CTEA is a rational enactment; we are not at liberty to second-guess congressional determinations and policy judgments of this order, however debatable or arguably unwise they may be. Accordingly, we cannot conclude that the CTEA […] is an impermissible exercise of Congress' power under the Copyright Clause".
[58] M.A. SINGER, *The Failure of the PRO-IP Act in a Consumer-Empowered Era of Information Production*, 43 Suffolk U. Law Review 185 (2009), 189, referring to Sony Corp. of America v.

One example of these deep modifications is the DMCA[59]. The Act was enacted in 1998 and deeply revised the 1976 Copyright Act to implement some provisions of the World Intellectual Property Organization (WIPO) Copyright Treaty (WCT) and the Performances and Phonograms Treaty (WPPT) adopted in 1996[60]. At the core of these treaties, and therefore at the core of DMCA, was the concern for the impact of digital technologies on the enforcement of copyright[61]. The Act, indeed, added three sets of rules, paired with civil remedies and criminal penalties, conceived as a remedy to the concerns of copyright owners and ISPs arising from the growth of the Internet[62]. Of the three sets of rules, the most interesting for our analysis is the one inserted in section 512 of Title 17[63], since it is related to the liability of ISPs. As it will be shown throughout the chapter, ISPs have played an important role in the history of peer-to-peer and the battle against it. Furthermore, DMCA introduced the "*subpoena duces tecum*" provision, which proved to be an important tool for the RIAA's cases against copyright infringement. For these reasons, the DMCA provisions will be here briefly analyzed.

In enacting the DMCA, Congress, as often happens, had to contemplate different interests: those of copyright owners and those of ISPs. As a consequence, the first title of the Act safeguards the interests of the former, while the second title

---

Universal City Studios, 464 U.S. 417 (1984), at 430 - for a summary of this seminal case see later in this chapter.

[59] For an overview of the impact of digital technologies on U.S. copyright law and a history of DMCA, see D. NIMMER, *Copyright: Sacred Test, Technology, and the DMCA*, The Hague, 2003.

[60] For a general overview and more references see D. NIMMER, *A tale of Two Treaties*, 22 Colum.-VLA J.L. & Arts 1 (1997). For a deep explanation of the two treaties see M. FICSOR, *The law of copyright and the Internet: the 1996 WIPO treaties, their interpretation, and implementation*, Oxford, 2002; J. REINBOTHE, S. VON LEWINSKI, *The WIPO Treaties 1996: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty: commentary and legal analysis*, London, 2002.

[61] C. WILDPANER, *The U.S. Digital Millennium Copyright Act. A Challenge for Fair Use in the Digital Age*, Vienna, 2004, 49 ff.; D. NIMMER, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 Cardozo L. Rev. 917 (2002).

[62] LAFRANCE, *Copyright Law in a Nutshell*, cit., 348. ISP is "a company that provides one of the permanent links that make up the Internet and sells connections to private users and companies to allow them to access the Internet", *Entry: ISP*, S.M.H. COLLIN, *Dictionary of Computing*, London, 2004.

[63] The other two sets of rules pertain the so called "anti-circumvention provisions" codified at § 1201 and prohibiting the circumvention of technological devices that copyright owner can apply to their digitalized products in order to protect them from unauthorized access or copying; and those codified at § 1202, which prohibit the falsifying or unauthorized alteration or removal of certain information attached to or accompanying a copyrighted work. For an overview see LAFRANCE, *Copyright Law in a Nutshell*, cit., 362 ff. As for remedies, § 1204(a) punishes with fines and even imprisonment who willfully violates §§ 1201 and 1202.

provides liability limitations for the latter[64]. According to its legislative history, the whole section was "intended to preserve incentives for online service providers and copyright owners to cooperate and detect and address copyright infringement that occur in the digital networked environment"[65].

Paragraph 512, also named *Online Copyright Infringement Liability Limitation Act* (OCILLA)[66], defines the so-called "safe harbor" provisions, which limit Online Service Providers' (OSPs) liability for the infringing activity of their users[67]. The conditions for satisfying section 512 safe harbors are different for different Service Provider functions. There are four main activities: section 512(a): transmission; section 512(b): system caching; section 512(c): storing of material at a user's direction: section 512(d): providing information location tools. Each of these sections provides for a different level of protection against liability, which is indeed connected to the particular activity that gave rise to the potential liability[68]. The failure to qualify for any of these safe harbors does not affect other possible defenses for ISPs, which therefore could nonetheless be found not liable for other reasons[69].

We can quickly describe these activities as follows[70]:

a) Transmission: the ISP only acts as a data conduit, transmitting information from one point on a network to another, following someone else's request[71];

[64] History has shown that ISPs, as "deep pockets" subjects, have been targeted far and wide by copyright holders in copyright infringement cases, dating back to 1993 (see *Playboy Enterprises, Inc., v. Frena*, 839 F. Supp. 1552 (MD Fla. 1993); the cases told in this paragraph are just some other examples. For an idea of "deep pockets" theory see G. CALABRESI, *The Costs of Accidents: A Legal and Economic Analysis*, New Haven, 1970, 40 e ss.

[65] 144 Cong. Rec. S11890 (ed. Oct., 8, 1998) – Statement of senator Leahy, available at: http://www.gpoaccess.gov/crecord/98crpgs.html.

[66] 17 U.S.C. § 512; see S.E. HALPERN, *New Protections for Internet Service Providers: An Analysis of "The Online Copyright Infringement Liability Limitation Act"*, 23 Seton Hall Legis. J. 359 (1999).

[67] More precisely, the Act provides safe harbors from monetary damages for ISP under some given circumstances. Therefore an ISP may still be subject to injunctive remedies, see 17 U.S.C. § 512(a)(1), (b)(1), (c)(1), (d)(1); see HALPERN, *New Protections for Internet Service Providers: An Analysis of "The Online Copyright Infringement Liability Limitation Act"*, cit., 387 ff. See also LAFRANCE, *Copyright Law in a Nutshell*, cit., 348 ff.;

[68] C. ANDREPONT, *Digital Millennium Copyright Act: Copyright Protection for the Digital Age*, 9 DePaul-LCA J. Art & Ent. L. 420, 412 ff. (1999).

[69] LAFRANCE, *Copyright Law in a Nutshell*, cit., 349.

[70] For the following explanation I will rely on the U.S. COPYRIGHT OFFICE, *Summary of The Digital Millennium Copyright Act of 1998*, 8 ff., available at: www.copyright.gov/legislation/dmca.pdf [DMCA SUMMARY].

[71] "This limitation covers acts of transmission, routing, or providing connections for the information, as well as the intermediate and transient copies that are made automatically in the operation of a network", DMCA SUMMARY, 10.

b) System caching: the provider retains copies, for a limited period, of material made available online by another person, and then transmitted to a subscriber at her direction[72];

c) Storing of material: the provider hosts on her system material websites or other information repositories, where material is stored at user's direction [73];

d) Providing information-location tools: it occurs when the ISP supplies users with a reference or a link to a site containing the requested material[74].

Safe harbors of sections 512(b), (c) and (d) require ISPs to be unaware of the infringing activity and to promptly remove or disable access to infringing material, upon receiving a notice of claimed infringement. This provision is usually referred to as the "notice and take-down" procedure. To be effective, the notice must meet some requirements provided by section 512(c)(3)[75]. If lacking one or more requirements, the notice will not be considered in determining whether the provider was aware or not of the infringing circumstances in the case of sections 512(c) and (d). If an ISP qualifies for a safe harbor, it is not liable for any monetary relief. This means that it is exempted from damages, costs, attorneys' fees and any other monetary payment. In addition, the ISP is not subject to injunctions or other equitable reliefs[76].

[72] Acting this way the ISP can fulfill other request of the same material just transmitting the retained copy, instead of retrieving the material directly from the original source, DMCA SUMMARY, 10.

[73] DMCA SUMMARY, 11.

[74] Search engines are an example, DMCA SUMMARY, 12.

[75] § 512(c)(3) *Elements of Notification*: A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following: (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site. (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material. (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted. (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law. (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

[76] There are nonetheless some limits to this liability restrictions, cf. LAFRANCE, *Copyright Law in a Nutshell*, cit., 359-361.

This part of DMCA was the outcome of a long negotiation between copyright owners and ISPs[77]. As a result, Congress created a sort of trade-off: service providers could receive liability protection in exchange for assisting copyright owners in the identification of infringers[78]. In order to encourage this cooperation, section 512(h) introduced the mentioned subpoena: "[a] copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer".

In order to better understand the provision, it is worth explaining that a subpoena is a discovery device that emanates from a court and orders a person (other than the parties) to attend, for example, a trial and give testimony or to produce a document or other information[79]. Section 152(h) provision introduces a "*subpoena duces tecum*", which is a judicial process by which the court, at the request of a party, commands to a third person the production of papers, documents, or other tangible items of evidence at the trial[80]. As will be seen, this rule has proven to be of absolute importance in more than one lawsuit contraposing the RIAA and ISPs, as it will be later demonstrated in this chapter[81].

An important amendment to the *Copyright Act* was made in 1997 with the promulgation of the *No Electronic Theft Act* (NET Act)[82]. This Act was aimed (also)

[77] According to *In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 773 (8th Cir., 2005).
[78] See *In re Verizon Internet Services*, 240 F. Supp. 2d 24 (D.D.C. 2003), 37.
[79] Fed. R. Civ. P. 45(a). See R.D. FREER, *Civil Procedure*, New York, 2009, 367 ff.; see *Entry: Subpoena*, H.C. BLACK, *Black's Law Dictionary*, St Paul, 1979, 1279.
[80] *Entry: Subpoena duces tecum,* BLACK, *Black's Law Dictionary*, cit., 1279. Nowadays one can gain the production of documents from a nonparty directly with a subpoena. This was once possible only through a *subpoena duces tecum*, which required the nonparty to attend the trial and to bring the required documents. The nonparty should then swear and be asked if she brought the documents. Once she identified the documents, her deposition would finish and the party could inspect the documents. The procedure is now easier, since the party can merely serve the nonparty with a subpoena for production of the materials. There is no more need to go through the process of noticing her deposition. See FREER, *Civil Procedure*, cit., 374-375.
[81] The subpoena introduced with DMCA has been criticized for many reasons: some of them will be explored later in this chapter. This controversial tool has been re-considered in a Bill that would have provided some protection for ISPs against the subpoena. The proposal would have blocked subpoenas, except in already pending civil lawsuits and when unauthorized copies of copyrighted works were stored on websites. Some have claimed that the Bill would have been more an "anti-RIAA" or "pro-P2P" provision than a real challenge to the current DMCA subpoena. Cf. R.J. DELCHIN, *Musical Copyright Law: Past, Present and Future of Online Music Distribution*, 22 Cardozo Arts & Ent. L.J. 343 (2004), 394.
[82] An Act of December 16, 1997, Pub. Law 105-147, 111 Stat. 2678 - To amend the provisions of titles 17 and 18, United States Code, to provide greater copyright protection by amending criminal copyright infringement provisions, and for other purposes.

to increasing the criminal provisions applied to copyright infringement. Indeed, the *Copyright Act* of 1976 had already some provisions punishing those who "willfully and for purposes of commercial advantage or private financial gain" infringed copyright[83]. Furthermore, in 1982, Congress increased the criminal penalties for the reproduction or distribution of sound recordings and other audiovisual works[84]. In 1992, the *Copyright Felony Act* entered into force[85], which brought felony penalties for all categories of copyright infringement[86].

The NET Act amended several sections of Title 17 and erased the requirement that the infringement had to be made for commercial advantage or financial private gain[87]. The NET Act modified the definition of "financial gain" contained in section 101, which now comprises "receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works". Criminal penalties were raised and range from one year to five years in prison, depending on the value of copyrighted works' copies distributed and on the financial gain[88]. The Act attracted a lot of criticism[89], even if Congress had emphasized that the new statute would punish only those who had acted intentionally[90].

For what is more strictly related to file-sharing, the US has enacted specific statutes to fight against this alleged plague. More than one bill has been proposed to target individual file sharers and/or file sharing technologies and their producers.

---

[83] Title 17 U.S.C. § 506(a).

[84] "Thus, under the 1982 legislation, criminal penalties for the unauthorized reproduction or distribution of at least sixty-five copies of a motion picture, or at least one hundred copies in the case of sound recordings, within a 180-day period were increased to a maximum fine of $250,000, up to five years in prison, or both" – S.A. SHAYESTEH, *High-Speed Chase On The Information Superhighway: The Evolution Of Criminal Liability For Internet Piracy*, 33 Loyola Of Los Angeles Law Review 183 (1999), 201. Cf. 18 U.S.C. § 2318.

[85] An Act of October 28, 1992, Pub. Law 102-561, 106 Stat. 4233.

[86] SHAYESTEH, *High-Speed Chase On The Information Superhighway*, cit., 202.

[87] It seems that this Act is a response to the case *United States v. LaMacchia*, 871 F. Supp. 535 (1994), stating that infringers could not be prosecuted under the Copyright Act for electronic copyright infringement if they did not realize commercial advantage or private financial gain. This would have created a loophole, since copyright infringers could not be held liable unless it was shown that they had profited financially from that infringement. Cf. SHAYESTEH, *High-Speed Chase On The Information Superhighway*, cit., 204.

[88] Cf. Title 18 § 2319.

[89] See for example SHAYESTEH, *High-Speed Chase On The Information Superhighway*, cit., 222 ff.; A. GROSSO, *Legally speaking: the promise and problems of the No Electronic Theft Act*, 43 Communications of the ACM 23 (2000).

[90] "[T]he bill […] has new language which makes it clear that there is no effort here and no intention on our part to make it easier to go after people when they were not acting intentionally" - 143 Cong. Rec. H9883 (ed. Nov., 4, 1997) – Statement of Representative B. Frank, available at http://www.gpo.gov/fdsys/pkg/CREC-1997-11-04/pdf/CREC-1997-11-04-pt1-PgH9883.pdf.

Some of these bills will be here described, even if they are just some examples of the many attempts that the legislative branch has made to stop file sharing[91].

Inducing Infringement of Copyrights Act[92], often cited as INDUCE Act, of 2004 is one of these bills. The Act would add a subsection (g)(1) to section 501 of Title 17, inserting an "intentional inducement" of any violation of the exclusive rights of the copyright owner (sections 106-122) and punishing those who intentionally aid, abet, induce, counsel, or procure this infringement. The "intent" could be shown by "acts from which a reasonable person would find intent to induce infringement based upon all relevant information about such acts then reasonably available to the actor, including whether the activity relies on infringement for its commercial viability". The amendment explicitly states that no modification would be brought to the doctrines of vicarious and contributory liability for copyright infringement.

The Bill was somehow a consequence of the *Grokster* decision, in which the inferior courts held that the providers of software that enable users to exchange copyrighted material were not liable, because they had not the ability to control users[93]. The Bill was highly criticized, since it seems to undermine innovation[94]. In fact, the idea behind the Bill was to target P2P companies, liable to induce users in file sharing, as it was later decided by the Supreme Court in the *Grokster* case[95]. Some argued that this Bill would overrule the famous *Sony Betamax* decision[96]. This would likely depend on the very interpretation of the words by courts, linked to the facts of an actual case. The wording of the amendment would have likely brought

[91] To get an idea of how many different bills related to intellectual property are pending in front of the US Congress see http://en.wikipedia.org/wiki/List_of_intellectual_property_legislation_pending_in_the_United_States_Congress (which is nevertheless an incomplete list!).

[92] S. 2560, 108th Congress, 2d Session – An Bill to amend chapter 5 of title 17, United States Code, relating to inducement of copyright infringement, and for other purposes, available at http://www.gpo.gov/fdsys/pkg/BILLS-108s2560is/pdf/BILLS-108s2560is.pdf.

[93] *MGM Studios, Inc., v. Grokster, Ltd*, 259 F.Supp. 2d 1029 (C.D. Cal. 2003) and *MGM Studios, Inc., v. Grokster, Ltd*, 380 F.3d 1154 (9th Cir. 2004) for which see later in this chapter.

[94] See for example J. SCHULTZ, *The False Origins of the Induce Act*, 32 Northern Kentucky Law Review 527 (2005); M. RAUCCI, *Congress wants to give the RIAA control of your IPod: how the INDUCE Act chills innovation and abrogates* Sony, 4 John Marshall Rev. Intellectual Property Law 534 (2005).

[95] *MGM Studios, Inc., v. Grokster, Ltd*, 545 U.S. 913 (2005), for which see below.

[96] The decision to which I am referring is Sony Corp. of America v. Universal City Studios, 464 U.S. 417 (1984); for an account of it, see *infra*. See SCHULTZ, *The False Origins of the Induce Act*, cit., 540 ff.

some problems, also due to its reference to the "reasonable person standard"[97]. Nevertheless, in the proposer's view this amendment could have stopped, or at least reduced, illegal file-sharing[98].

In 2003 a bill was proposed specifically to stop P2P, as the name "*Peer-to-peer Piracy Prevention Act*" suggests[99]. The Bill would have modified section 514 of the *Copyright Act* to protect copyright owners from legal actions that could arise from "blocking, diverting or otherwise impairing the unauthorized distribution, display, performance, or reproduction of his or her copyrighted work on a publicly accessible peer-to-peer ("P2P") file trading network". It would have create a safe harbor shielding copyright owners from liability, for example for users' computer damages, linked to actions designed to prevent the unauthorized distribution of their works to the public through P2P technologies. Whenever a copyright holder wanted to stop the distribution of her works, she would notify the Attorney General of the method she wanted to apply and, upon request, provide also the rights and reasons behind this action[100]. The Bill would have brought with it more than one problem, due in part to the breadth and the unclear wording of the safe harbor provision[101]. However, the Bill never became law.

Later two other bills were proposed: the *Piracy Deterrence and Education Act* and the *Protecting Intellectual Rights Against Theft and Expropriation Act* (PIRATE Act)[102]. The PIRATE Act was passed in Senate on June 2004 and would

---

[97] The broad wording of the Bill could have created a constitutional problem, inducing courts to decide whether a technology was appropriate or not, see RAUCCI, *Congress wants to give the RIAA control of your IPod: how the INDUCE Act chills innovation and abrogates* Sony, cit., 549.

[98] See J.C. TWU, *Inducing Infringement of Copyrights Act of 2004: FindLaw Interview with John Hughes and Jennifer M. Rich of Townsend and Townsend and Crew LLP*, available at http://library.findlaw.com/2004/Sep/27/133584.html.

[99] H.R. 5211, 107th Congress, 2d Session – A Bill to amend title 17, United States Code, to limit the liability of copyright owners for protecting their works on peer-to-peer networks, available at http://www.gpo.gov/fdsys/pkg/BILLS-107hr5211ih/pdf/BILLS-107hr5211ih.pdf.

[100] H.R. 5211, 107th Congress, 2d Session, cit., § 514(a)-(c).

[101] For an account of the potential problems associated with this Bill see J.S. HUMPHREY, *Recent Development: Debating the Proposed Peer-to-Peer Piracy Prevention Act: Should Copyright Owners be Permitted to Disrupt Illegal File Trading Over Peer-to-Peer Networks?*, 4 North Carolina J. of Law & Technology 375 (2003), 380 ff.

[102] Respectively H.R. 4077, 108th Congress, 2d Session – An Act to enhance criminal enforcement of the copyright laws, to educate the public about the application of copyright law to the Internet, and for other purposes, available at http://www.gpo.gov/fdsys/pkg/BILLS-108hr4077rds/pdf/BILLS-108hr4077rds.pdf; and S. 2237, 108th Congress, 2d Session – An Act to amend chapter 5 of title 17, United States Code, to authorize civil copyright enforcement by the Attorney General, and for other purposes, available at http://www.gpo.gov/fdsys/pkg/BILLS-108s2237rfh/pdf/BILLS-108s2237rfh.pdf.

have authorized the Justice Department (i.e. Attorney General) to file civil lawsuits against infringers, instead of leaving to copyright holders the possibility of initiating and action[103]. This Act was meant as an amendment to the previous NET Act. Indeed, even if NET had already stated that the Justice Department could bring criminal charges against infringers, due to some technicalities, such as the high burden of proof, no single criminal case against file sharers had been filed in the first years after the Act passed[104]. The PIRATE Act would have avoided this problem, given that the Department of Justice could directly bring civil suits, with a lower burden of proof[105]. Eventually the Act failed to pass at the House Committee on the Judiciary. Variations of the same Act have been proposed, but none of them has yet been approved[106].

The *Piracy Deterrence Education Act* was also proposed in 2004. Under this Act, file sharers who offered "for distribution to the public" more than 1000$ of copyrighted materials would have been punished with prison (up to three years) and with fines up to 25,000$[107]. Together with these criminal penalties, the Act would have lowered the burden of proof for criminal prosecution. The Bill was intended to finally punish file-sharers criminally, who previously could not be pursued criminally since they had not distributed copyrighted works for financial gain[108]. The Act never became law.

After these failed attempts, the Congress finally enacted the *Prioritizing Resources and Organization for Intellectual Property Act* (PRO-IP Act) of 2008[109]. The Act has been called "a culmination of all [the] historical, legislative, and

[103] Cf. F. TABATABAI, *A Tale of Two Countries: Canada's Response to Peer-to-Peer Crisis and What It Means for the United States*, 73 Fordham Law Review 2321 (2005), 2355.
[104] Cf. D. MCCULLAGH, '*Pirate Act' raises civil rights concerns*, CNETNews.com, May 26, 2004 available at http://news.cnet.com/'Pirate-Act'-raises-civil-rights-concerns/2100-1027_3-5220480.html, reporting that "[t]he Justice Department has indicated that it won't target peer-to-peer networks for two reasons: Imprisoning file-swapping teens on felony charges isn't the department's top priority, and it's always difficult to make criminal charges stick."
[105] TABATABAI, *A Tale of Two Countries*, cit., 2356.
[106] See for example the *Intellectual Property Enforcement Act* of 2007 – A bill to amend titles 17 and 18, United States Code, and the Trademark Act of 1946 to strengthen and harmonize the protection of intellectual property, and for other purposes, 110th Congress, 1st Session, S. 2317, available at http://www.gpo.gov/fdsys/pkg/BILLS-110hr3578ih/pdf/BILLS-110hr3578ih.pdf.
[107] Cf. § 110(a) of the Bill.
[108] TABATABAI, *A Tale of Two Countries*, cit.,, 2357.
[109] An Act of October 13, 2008, Pub. Law. 110–403, 122 STAT. 4256 – To enhance remedies for violations of intellectual property laws, and for other purposes.

executive developments of criminal IP law"[110]. The initial draft of the Bill had a provision that would have allowed the Attorney General to file civil actions on behalf of the allegedly damaged party. However this provision was thought to be too severe and it was cancelled. Nevertheless, the whole Congress felt the necessity to prosecute infringers with criminal sanctions, in order to deter their unlawful behavior[111]. Therefore, the Act expressly designated copyright infringement as a "felony", replacing the milder term of "offense"[112]. It also created an Intellectual Property Enforcement Coordinator (IPEC), who is appointed by the President, whose task is to oversee an interagency IP enforcement advisory committee that should develop a "joint strategic plan" for the enforcement of intellectual property[113]. As one could imagine, this Act was criticized. In particular it has been said that it broke the boundaries between civil and criminal IP law. Furthermore, this statute failed to address the problem of the increasingly widening distance between the social perception of copyright infringement and the legal consideration of the same[114]. In other words, it does not take into account the social norms currently governing (digital) copyright infringement. The Act also seems to have totally disregarded the need for a balance between copyright holders and copyright users[115].

More recently other two bills were introduced in the House of Commons and in the Senate: there are respectively entitled *Stop Online Piracy Act* (SOPA)[116] and *PROTECT IP Act* (PIPA)[117]. SOPA was thought to give more enhance law

[110] G. PYUN, *The 2008 Pro-IP Act: The Inadequacy Of The Property Paradigm In Criminal Intellectual Property Law And Its Effect On Prosecutorial Boundaries*, 19 DePaul J. Art Tech. & Intell. Prop. L. 355 (2009), 373.
[111] PYUN, *The 2008 Pro-IP Act*, cit., 374.
[112] The Act also extends the provisions related to civil and criminal forfeiture.
[113] SINGER, *The Failure of the PRO-IP Act in a Consumer-Empowered Era of Information Production*, cit., 199.
[114] PYUN, *The 2008 Pro-IP Act*, cit., 379 ff.; SINGER, *The Failure of the PRO-IP Act in a Consumer-Empowered Era of Information Production*, cit., 209.
[115] Cf. PYUN, *The 2008 Pro-IP Act*, cit., 388: "[t]he ultimate purpose of IP law is to preserve the balance between public access and IP owner rights, and the PRO-IP Act demonstrates Congress's pro-IP industry policies".
[116] A Bill to promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes. 112th Congress, 1st Session, H. R. 3261, available at: http://www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih/pdf/BILLS-112hr3261ih.pdf.
[117] Entire title: *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*, A Bill to prevent online threats to economic creativity and theft of intellectual property, and for other purposes, 112th Congress, 1st Session, S. 968, available at: http://www.gpo.gov/fdsys/pkg/BILLS-112s968is/pdf/BILLS-112s968is.pdf.

enforcement to fight online trafficking of copyrighted materials and counterfeit goods. Among the provisons was the possibility to ask a Court to order an ISP to block access to the website. It would have also expanded existing criminal laws, including streaming of copyrighted contents, imposing prison as penalty. PIPA was similar to SOPA and aimed at giving US government and copyright holders additional tools against online threats to copyrighted materials. The bill was thought again to enhance enforcement especially against rogue websites operated and registered overseas.

Both the bills gave rise to widespread protests against what users called "internet censorhip"[118]. This worldwide disapproval, supported by some website voluntary blackouts[119], led both the Senate and the House to indefinitely delay the vote for both the bills[120].

The trend to enlarge the province of copyright, to enhance its enforcement tools, and meanwhile, to lessen and reduce users' rights does not seem to stop. This is shown not only by the bills here recalled, but also from some judicial interpretation, as it will be demonstrated throughout this work.

2.2 The legal framework of information privacy

Just as every classical treatise on US copyright starts with mentioning Clause 8 of the Constitution, every classical discussion on US privacy begins with the introduction to the seminal article by Warren and Brandeis "*The Right to Privacy*"[121]. The piece is probably "the most important article ever written about privacy"[122].

---

[118] See for example J. VIJAYAN**,** *Protests against SOPA, PIPA go viral. Google, Wikipedia, Reddit, BoingBoing plan unprecedented Internet 'strike' Wednesday*, Computerworld.com, January 17, 2012, at: http://www.computerworld.com/s/article/9223496/Protests_against_SOPA_PIPA_go_viral.

[119] I am making reference in particular to Wikipedia: J. MITCHELL, *Wikipedia: So How Do You Like Censorship?*, readwriteweb.com, January 19, 2012, available at: http://www.readwriteweb.com/archives/wikipedia_so_how_do_you_like_censorship.php.

[120] D. COPELAND, *SOPA, PIPA Votes Indefinitely Delayed*, readwriteweb.com, January 20, 2012, at: http://www.readwriteweb.com/archives/sopa_pipa_votes_indefinitely_delayed.php.

[121] WARREN, BRANDEIS, *The Right to Privacy*, cit.,spec. 198 ff., where the authors make a parallel between individual privacy and the protection of ideas and thoughts or of works of art (eventually combining privacy and copyright). My narration of the right to privacy history and framework will necessarily be brief, given the goal of this work. For a thorough analysis of the issue and further bibliography see, among others, D.J. SOLOVE, P.M. SCHWARTZ, *Privacy, Information, and Technology*, New York, 2009, 10; D.J. SOLOVE, P.M. SCHWARTZ, *Information privacy law*, New York, 2009; D.J. SOLOVE, M. ROTENBERG, *Information privacy law*, New York, 2003; J.T. SOMA,

The origins of this influential paper have been deeply analyzed by many scholars. One of the most accredited versions is that which concerns the introduction of a new technology. Warren and Brandeis were indeed worried that "yellow" journalism would become even more intrusive thanks to the invention of portable cameras, which could take instantaneous pictures. With this camera people could take pictures in public places more easily. This meant that newspapers could start putting pictures in their editions, finally abandoning drawings[123]. In particular, it seems that the writing was inspired by the intrusion of journalists in the private life of Samuel Warren. He was a powerful and rich attorney of Boston and practiced with Brandeis (who eventually later became a Supreme Court Justice). Furthermore, Warren's wife was the daughter of a famed senator from Delaware. Many authors claim that Warren's impetus for writing the article came from his displeasure related to what was published in newspaper about his social life[124].

Whichever origins this article had, the authors referred to privacy as "the right to be let alone"[125], suggesting the introduction of an action in tort and an injunction as remedies for its protection. Indeed, the contents of the article suggested that the existing common law could not protect privacy and that law could, and ought to, intervene to reach this aim. Courts did not wait. Already at the beginning of the twentieth century they began introducing a number of privacy torts to fill the gaps that the two authors had identified[126]. The interventions of judges never ceased and eventually led to another seminal article by William Prosser[127].

S.D. RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, St Paul, 2008. See also WESTIN, *Privacy and Freedom*, cit., spec. 330 ff. For a deep analysis of the historic development of privacy in USA see F.S. LANE, *American Privacy. The 400-Year History of Our Most Contested Right*, Boston, 2010.

[122] SOLOVE, SCHWARTZ, 10. The authors report that in the Supreme Court case *Kyllo v. United States*, 533 U.S. 27 (2001), Warren and Brandeis' article was cited by the majority, by judges who concurred in the opinion and even by those who were dissenting.

[123] WARREN, BRANDEIS, *The Right to Privacy*, cit., 195-196. It was the Snap Camera by Kodak, SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 11; WESTIN, *Privacy and Freedom*, cit., 338 and 344 ff. For the different explanations related to Warren and Brandeis' article origins, see *Ibidem*, 11-12.

[124] SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 12; W. PROSSER, *Privacy*, 48 California Law Review 383 (1960), 383. For an analysis of how the increasing use of technology heighted first the fear and then the awareness of the need for privacy see WESTIN, *Privacy and Freedom*, cit., 298 ff. Warren and Brandeis wrote that privacy was a modern right for men and women, arising from the modern society (cf. WARREN, BRANDEIS, *The Right to Privacy*, cit., 196) . Westin disagrees, basing his argumentation on history. Cf. WESTIN, *Privacy and Freedom*, cit., 337.

[125] WARREN, BRANDEIS, *The Right to Privacy*, cit., 195.

[126] SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 25-26 cite some cases, among which *Roberson v. Rochester Folding Box Co*., 64 N.E.. 442 (N.Y. 1902). As a consequence to this

By analyzing more than three hundreds privacy cases decided since Warren and Brandeis' publication, Prosser extracted four different categories of torts, which were later introduced in the *Restatement of Torts*. The idea of Prosser's was that the extreme confusion on privacy and its protection was due to a failure in distinguishing these forms of torts[128]. The four torts are collectively known as "invasion of privacy" and include: intrusion upon seclusion, public disclosure of private facts, false light and appropriation[129]. In particular, according to the *Restatement (Second) of Torts*, the four privacy torts can now be described as follows:

1. *Public disclosure of private facts*: is the act of giving publicity to facts or acts regarding a person, which are embarrassing and which were otherwise not so widely known. This tort can be broken down into four elements: dissemination of true information (1), offensive to a reasonable person (2), not of public concern (3) and so intimate that it collides with the public's sense of decency (4)[130].

2. *Intrusion upon seclusion*: is the only one of the four privacy torts which does not require publicity. It is the gathering of information in someone's private space. The wrongdoing occurs at the time of the intrusion, not at the moment of the publication of the gathered personal information. It is an invasion of one's private affairs or solitude. The intrusion does not need to be physical, but it can be also visual or audio[131];

---

decision, which asked for the intervention of the legislative body, New York state introduced a privacy tort action by statute. See also *Pavesich v. New England Life Insurance Co*., 50 S.E. 68 (Ga. 1905), which, according to Solove and Schwartz, made Georgia the first state to recognize a common law tort action for privacy invasion. Both the mentioned cases involved the publication of plaintiff's image without consent.

[127] PROSSER, *Privacy*, as above cited.

[128] PROSSER, *Privacy*, cit., 407.

[129] PROSSER, *Privacy*, cit.,389 ff. Prof. Solove criticizes Prosser's classification and proposes an expansion of the protection of privacy beyond tort law. Solove claims that privacy is a vague concept, often invocated for situations which vary deeply one from the other. Solove suggests a variety of solutions each directed to a different understanding of "privacy", better tailored to the new landscape created by digital technologies, which did not exist when Prosser proposed his vision. See SOLOVE, *A Taxonomy of Privacy*, cit. The author proposes a taxonomy of four groups of harmful activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion, each of which comprises more different harmful situations. See *Ibidem*, 488 ff.

[130] The American Law Institute, *Restatement (Second) of Torts*, 1977, § 652D – "Publicity Given to Private Life" [*Restatement (Second) of Torts*]. SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 38 ff. This figure of privacy tort is the one that most closely collides with freedom of speech and press protected by the First Amendment. See PROSSER, *Privacy*, cit., 392-398.

[131] *Restatement (Second) of Torts*, § 652B – "Intrusion upon Seclusion". See SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 41 ff. Cf. PROSSER, *Privacy*, cit., 389-392.

3. *False light*: this figure of tort is close to defamation and concerns an individual who is put under a "false light" in the eye of the public, for example through the publication of misrepresenting facts, which are normally highly offensive. According to the *Restatement (Second) of Torts*, the offensiveness of false light has to be evaluated from a reasonable point of view and the actor had to undertake the publication with knowledge or with reckless disregard[132];

4. *Appropriation*: aims at preventing unjust enrichment deriving from the theft of ones' name or likeness[133].

Privacy is also protected by other torts, such as "breach of confidentiality", that provides a remedy for the case in which a professional discloses a patient or a client's confidential information; "defamation", consisting in the tort of libel and slander, under which a person is liable when makes false statements about a person and harms her reputation; and "infliction of emotional distress" which provides a remedy when a person "by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another"[134].

Obviously, privacy is not only a matter of private law, but it touches more or less deeply upon other branches of law. In fact, although the US Constitution never specifically mentions privacy, courts and scholars have extracted its protection from a number of different constitutional provisions[135]. In particular, constitutional privacy

[132] *Restatement (Second) of Torts*, § 652E – "Publicity Placing Person in False Light". Cf. SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 35 ff. See also PROSSER, *Privacy*, cit., 398-401.

[133] *Restatement (Second) of Torts*, § 652C – "Appropriation of Name or Likeness". See SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 32 ff. Cf. PROSSER, *Privacy*, cit., 401-407. Prosser explained that intrusion and disclosure require the invasion of something secret, secluded or private pertaining to the plaintiff, while false light and appropriation do not. Furthermore, disclosure and false light depend on publicity, while the other two do not, even if appropriation usually does. Of the four, only false light requires fiction or falsity and only appropriation implicates a use for the defendant's advantage; cf. PROSSER, *Privacy*, cit., 408.

[134] *Restatement (Second) of Torts*, § 46. The application of this tort is limited, due to the requirement of an "extreme and outrageous conduct". Cf. SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 31.

[135] Despite the Federal Constitution does not mention privacy, some states have provided for the protection of this right in their own constitutions. As an example let us report the Californian Constitution, which, at art. I, § 1 provides: "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*"(emphasis added). Other examples are art. I, § 22 of Alaska Constitution or art. I, § 23 of Florida Constitution. Cf. SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 170 ff. for state constitutions and statutes on privacy. It should be noted, however, that the "Congressional Findings and Statement of Purpose" of 1974 Privacy Act (for which see *infra*) state "the right to privacy is a personal and fundamental right protected by the Constitution of the United States"., cf. Section 2 - Pub. L. 93-579.

in the USA is generally understood as "the right of persons to be free from unwanted and unwarranted governmental intrusions"[136]. Despite the fact that many different approaches to privacy can be outlined from the Constitution, it seems that they can be all grouped under two main umbrellas: individual privacy or autonomy, on the one hand, and data privacy or control of information on the other[137].

One example of the constitutional approach to privacy is given by the First Amendment, which states: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances". Under this Amendment, people have a primordial right to speak anonymously[138]. Furthermore, the same Amendment can protect against compulsory disclosure of certain information, such as names and addresses of the members of an organization or the name of organizations to which public teachers belong[139].

The First Amendment is not the only piece of the Constitution which provides protection for privacy[140]. The Fourth Amendment requires that people "be secure in their persons, houses, papers, and effects, against unreasonable searches or seizure". It was Justice Brandeis himself that wrote an important dissenting opinion that had a significant influence on the interpretation of this Amendment. The decision was about the use of wiretapping which the majority held was not an invasion of privacy, since there was no physical trespass to home. Justice Brandeis' dissent put stress on the existence of that "right to be let alone", which had appeared in 1890 article from Warren and the same Brandeis. He claimed that the Amendments had a much greater scope than protecting against just physical intrusion, and that happiness, the pursuit

[136] SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 57.
[137] See SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 57 ff.
[138] See the famous case *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995), in which the Supreme Court held that an Ohio law prohibiting anonymous political literature was unconstitutional.
[139] SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 33, cite *NAACP v. Alabama*, 357 U.S. 449 (1958) with respect to the disclosure of organization's members' information and *Shelton v. Tucker*, 364 U.S. 479 (1960) regarding a law which required public teacher to tell which organizations they belonged to.
[140] The Third Amendment also protects privacy in a fashion. It holds: "No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law". The Fifth Amendment protects people against compulsory divulgation of information about themselves, through the so called "privilege against self-incrimination", stating "No person […] shall be compelled in any criminal case to be a witness against himself […]".

of which everybody is entitled, was to be found also in immaterial things. Justice Brandeis argued that Amendments conferred the right to be let alone, which was "the most comprehensive of rights and the right most valued by civilized men"[141].

This orientation towards privacy, despite being a dissenting opinion, was later very influential on the interpretation of the Fourth Amendment. In fact, in another seminal case (*Katz v. United States*), the US Supreme Court held that the Fourth Amendment "protects people, not places"[142]. Furthermore, in his concurring opinion, Justice Harlan set the standard for the "reasonable expectation of privacy". This test helps in understanding whether the Fourth Amendment applies or not. First of all, a person must have exhibited an actual subjective expectation of privacy and, second, the expectation has to be one that society is prepared to recognize as reasonable[143]. In the 1965 landmark case of *Griswold v. Connecticut*, the US Supreme Court determined that an individual has a constitutional right to privacy[144]. This right was to be found in those "penumbral" zones of freedom which derived from an expansive interpretation of the Bill of Rights. As articulated in this case, the privacy right was

[141] *Olmstead v. United States*, 277 U.S. 438 (1928), 478. Olmstead was a bootlegger who had been convicted of violating federal Prohibition laws. His conviction came from telephone wiretapping. Olmstead claimed that wiretapping was a violation of the Fourth or the Fifth Amendment, since they were for the protection not only of property but also of the individual in his liberty and private life. After having lost in front of both the federal trial judge and the appeals court, Olmstead asked for a decision by the Supreme Court. The Supreme Court held that neither the Fourth nor the Fifth Amendment provided protection against wiretapping, since there was no physical trespass.

[142] *Katz v. United States*, 389 U.S. 347 (1967). The case was on the legality of an FBI device which, attached to the outside of a telephone booth, could monitor conversation on gambling operations. The plaintiff Katz argued that, unlike the government opinion, the telephone booth was a constitutionally protected area. The Court held that physical trespass was not required for the Fourth Amendment to come into play, since that Amendment protects people and not places. The telephone bug constituted a violation of privacy and a search and seizure under the Fourth Amendment.

[143] Cf. *Katz v. United States*, cit., 361. As it usually happens with "reasonable standards", also in this case many problems arose, since "*Katz* itself provides no clear indication how the lower courts are to draw th[e] line", see R.G. WILKINS, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 Vand. L. Rev. 1077, 1089 (1987). See also G.A. ASHDOWN, *Legitimate Expectation of Privacy*, 34 Vand. L. Rev. 1289 (1981) and A. LIBEU, *What is a reasonable expectation of privacy?*, 12 W. St. U. L. Rev. 849 (1985). See also SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 99 ff.

[144] *Griswold v. Connecticut*, 381 U.S. 479 (1965). The case was initiated against a Connecticut statute which prohibited the prescription and use of contraceptives. Two doctors had opened a birth control clinic in New Haven, Connecticut. Shortly after the clinic was opened, both of them were arrested, tried, found guilty and finally fined. The decision was upheld also by the Appellate Division of the Circuit Court and by the Connecticut Supreme Court. Griswold therefore appealed to the US Supreme Court. The Supreme Court held that the Connecticut statute was a violation of marital privacy. This privacy right could be found in many fundamental constitution laws, which created penumbras of privacy. As a result the Connecticut statute was considered unconstitutional.

close to the one advocated by Warren and Brandeis[145]. The case involved a Connecticut law that prohibited the use of contraceptives, which was considered by the Supreme Court to be unconstitutional, since it affected one's intimate choices about sexual life. This case cleared the way for other important decisions related to decisional privacy and autonomy[146]. Some years later the Supreme Court extended the right to privacy also to its informational aspect, recognizing "the individual interest in avoiding disclosure of personal matters"[147].

Meanwhile, the growing importance and presence of technology created a social concern for privacy, which was itself reflected in the high degree of political attention paid to the phenomenon. In 1973 the United Stated Department of Health, Education, and Welfare reviewed the state of data processing in USA. As a result, the Department proposed a *Code of Fair Information Practices*, which is composed by five basic principles that should allocate rights and responsibilities in the collection and use of personal information[148]. The code's compilers reached some important conclusions and in particular their findings recommended that:

1. There must be no personal data record-keeping systems whose very existence is secret;

2. There must be a way for a person to find out what information about the person is in a record and how it is used;

[145] WESTIN, *Privacy and Freedom*, cit., 355. See the words of Justice Black in *Griswold v. Connecticut*, cit., 510.

[146] See for example the famous *Roe v. Wade*, 410 U.S. 113 (1973). In this case the Supreme Court struck down a Texas law on abortion. To reach this conclusion the Court made an analysis of the right to privacy. The Court found that the Fourteenth Amendment due process clause was to be considered an expression of personal liberty, a right to privacy. Furthermore it stated that "the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy"; cf. *Ibidem*, 153.

[147] *Whalen v. Roe*, 429 U.S. 589 (1977), 599. This case involved New York Statutes requiring reporting and storage of information related to drug prescriptions. Physicians were required to report some information, which was then stored in the Department of State. A group of patients, several doctors and two associations of physicians challenged this statute. The Supreme Court recognized for the first time a right to information privacy, on the base of two individual interests: one in avoiding disclosure of personal matters and another in independence of making certain important decisions. Nevertheless, the Supreme Court held that the New York statute need to remain valid and that the prescription of some drugs had to remain recorded, since the statute did not really constitute a threat to individual interest or to the US Constitution.

[148] See U.S. DEP'T. OF HEALTH, EDUCATION AND WELFARE, *Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens* (1973).

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent[149];

4. There must be a way for a person to correct or amend a record of identifiable information about the person;

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

The Code had a deep influence on the privacy laws which were later enacted[150].

The same kind of influence was exercised also by the Organization for Economic Cooperation and Development (OECD) Guidelines, as well as by the European Data Protection Directive, all of which greatly affected the development of privacy law worldwide[151]. The OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* set out eight key principles with the aim of personal information protection. The principles were therefore thought as a way to harmonize national privacy legislation or serve as a basis for the upcoming legislation in those countries which had not implemented specific laws yet. In particular, they "should [have been] regarded as minimum standards which [were] capable of being supplemented by additional measures for the protection of privacy and individual liberty". The Guidelines "apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or

[149] This aims at avoiding secondary uses of the collected data, which are uses not desired by the individual to whom the data refer. Cf. SOLOVE, *A Taxonomy of Privacy*, cit., 519.

[150] This code influenced both US and other nations' privacy laws; cf. M. ROTENBERG, *Fair Information Practises and The Architecture of Privacy (What Larry Doesn't Get)*, 2001 Stan. Tech. Law Rev. 1, available at http://stlr.stanford.edu/2001/02/fair-information-practices-and-the-architecture-of-privacy/, ¶ 42 ff. According to this author, the Code of Fair Information Practise influenced even the OECD Guidelines, see *Ibidem*, ¶ 44-47.

[151] SOLOVE, ROTENBERG, *Information privacy law*, cit., 713. The OECD Guidelines related to the handling of personal data can be found at http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html. It will be later seen how these principles, as well as the European privacy law, influenced also Canadian privacy protection. Actually, while developing its guidelines, the OECD worked closely with the Council of Europe, which was already drafting its own Convention on Privacy. They are indeed very close. Despite OECD principles are not binding, many of the signatory countries have incorporated these principles into their privacy laws; cf. SOLOVE, ROTENBERG, *Information privacy law*, cit., 714.

because of their nature or the context in which they are used, pose a danger to privacy and individual liberties"[152].

Given the importance of these principles and their influence on the laws of the systems here considered, it is worth giving a brief account of them. The first articulated principle is that of *collection limitation*, according to which there should be limits to the collection of personal data, that should be obtained only with lawful means and with the consent of the data subject, where appropriate. Second is the principle of *data quality*, which means that collected data should be relevant to a specific purpose, as well as being accurate, complete and updated. With regard to the purpose, the third principle claims that the aim of the collection should be settled at the beginning (*purpose specification* principle) and it is linked to the fourth one, which prescribes that data ought to be used only for the specified limited purposes and not for purposes other than the one for which they were gathered (*use limitation* principle). *Security* is the fifth principle and, as can be easily imagined, necessiates that collection and storage of data be done to reasonably prevent loss, theft or modification of records. At the same time there should be *openness* (the sixth principle), meaning that there is transparency with respect to the practises of handling data. The seventh principle of *individual participation* should furthermore permit the access, confirmation and demand for modification of personal data by the concerned subject. The last principle requires those who handle data to be responsible for complying with the listed principles, and it is in fact the principle of *accountability*[153].

With these stated principles in mind, beginning from 1970 the US Congress passed a number of statutes protecting privacy in many sectors of the so-called information economy. This legislation is characterized by many specific laws, each directed to a different aspect of social life, such as family, employment, health care

[152] See "*Scope of the Guidelines*" at the cited *url* in order to better understand their scope. In developing the principles, the OECD explained the necessity for them. In particular, since many countries part of the OECD were already implementing their own legislation on privacy protection, the Organization's concerns were related to the possibility of disparity in national legislation that could hamper the free flow of personal data across borders (which could have obviously been a problem for the economy).

[153] SOLOVE, ROTENBERG, *Information privacy law*, cit., 713-714.

and so on[154]. Not every piece of legislation aimed at protecting privacy, since some of them were conceived, for example, as a way to ease government collection of data or enforcement of law[155]. Parallel to federal laws, states have also passed statutes protecting privacy in many contexts. Nevertheless, none of them has ever enacted a general law protecting privacy in an all-encompassing manner, especially in the private sector[156]. Moreover, some of the federal statutes on privacy protection have been enacted as a consequence to a particular episode, usually a shocking event, generating a sectorial approach[157]. The existence of many different laws has been sometimes criticized, especially, but not exclusively, by scholars living in legal systems applying a more all-embracing approach for the protection of privacy[158]. The result is that, in the majority of daily situations, unlike what happens in Canada or in the European Union, usually no protection of privacy applies, except from the privacy torts or contractual agreements[159].

The most complete and wide of the US statutes on privacy is the *Privacy Act 1974*[160], which was a sort of response to the so-called "Watergate scandal" which led President Richard Nixon to resign from his office. It was enacted to provide citizens with some rights on their personal information stored in governmental record

[154] For a complete list of the statutes related to privacy see SOLOVE, SCHWARTZ, *Information privacy law*, cit., 36 ff. or SOLOVE, ROTENBERG, *Information privacy law*, cit., 23-24.

[155] One of the most recent of these statutes is the USA-PATRIOT (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*) Act of 2001, signed on October 26, "to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes" - Pub. Law 107-56, 11 Stat. 271. See below.

[156] SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 38.

[157] SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 48. See also J. SOVERN, *Opting in, opting out, or no options at all: the fight for control of personal information*, 74 Washington Law Review 1033 (1999), 1042: "Laws regulating personal information […] are a patchwork of *ad hoc* responses to outrage over past invasions of privacy rather than a coherent set of rules based on fundamental principles and policies".

[158] See, for example, SOVERN, *Opting in, opting out, or no options at all: the fight for control of personal information*, cit., 1042. Another scholar claimed that "[t]his piece-meal approach to personal data protection makes it impossible for an individual to know her privacy rights" and therefore suggested the adoption of a more comprehensive approach for the private sector; see J.D. BLACKMAN, *Proposal For Federal Legislation Protecting Informational Privacy Across The Private Sector*, 9 Santa Clara Computer & High Tech. L. J. 431 (1993), 456. For his proposal, based on the draft of what later would become European Directive 95/46/EC; see in particular 465 ff.

[159] Note that not all privacy torts are recognized in every state. Cf. SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 48.

[160] An Act To amend Title 5, United States Code, by adding a Section 552a, to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies, to establish a Privacy Protection Study Commission, and for other purposes - U.S.C. § 552a - Pub. Law No. 93-579, 88 Stat. 1896 - December 31, 1974.

systems, including the right to see one's record and the right to modify it when inaccurate[161]. Congress thought this statute was a way for individuals to control and manage their personal information, which were under threat due to the increasing use of computers and other information technologies in the hands of the Government. In fact, the Act does not apply to private entities or business organizations; it applies only to public agencies and, more precisely, it applies only to federal ones and not to state or local agencies. To claim a *Privacy Act* violation, a plaintiff must prove that the information disclosed was a record, which must contain information about an individual and must be contained in a "system of records"[162]. Information can be kept only if it is relevant and necessary to accomplish the purposes of the agency; whenever an individual asks for explanation about the use of her information, agencies shall inform her. As already mentioned, every individual can access her records and ask for their modification in case of inaccuracies. Disclosure of such information to any person or to another agency is subject to the individual's own consent. There are exceptions related, for example, to law enforcement or to the sharing of information among federal agencies, but only as long as it is related to civil or criminal law enforcement. The broadest exception is nevertheless the "routine use" one: whenever disclosure is compatible with the purposes for which the agency that initially collected the record, the information can be disclosed to federal another agency without the consent of the person to whom this information is related[163].

Another important exception is related to the application of the *Freedom of Information Act* (FOIA): when the FOIA requires that records be released, the *Privacy Act* does not apply[164]. FOIA is an act that permits the access of the public to

[161] SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 304.
[162] Cf. § 552a(a)(4): "the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph"; and § 552a(a)(5)(5): "the term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual".
[163] Cf. § 552a(b)(3). There are conditions of disclosure listed in § 552a(b)(1)-(12) as well as in §§ 552a(k) and 552a(j).
[164] Cf. § 552a(k)(1).

governmental records[165]. It gives all persons the right to inspect and copy records maintained by any federal agency. FOIA itself contains some exemptions, two of which are "privacy related". One exempts from disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy", while the other one exempts from disclosure "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information […] could reasonably be expected to constitute an unwarranted invasion of personal privacy"[166]. Given this combination of exemptions, and in particular in the light of the interaction between the *Privacy Act* and FOIA, if a FOIA exemption on privacy applies, then the *Privacy Act* requires the Government to refrain from disclosing certain records[167].

Prior to the enactment of the *Privacy Act*, another influential Act had been passed. The *Fair Credit Reporting Act* of 1970 legislated on the use and disclosure of citizens' personal information handled by credit reporting agencies[168]. Due to the increase of purchases based on credit, credit reporting agencies got a great role in economic transactions. This Act was an answer to the lack of responsiveness of credit agencies to consumer complaints. In particular, the purpose of the Act was to "insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy"[169]. Many measures were introduced with this statute, such as limitations on the information which credit agencies can provide in their credit reports. Moreover, investigative

[165] Pub. Law 89-554, 80 Stat. 383 – July 4, 1966 – 5 U.S.C. § 552.
[166] Cf. § 552(b)(6) and § 552(b)(7)(C). For more details see SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 249 ff.
[167] SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 322. For an analysis of the mentioned exemption and further bibliography see A.T. KRONMAN, *The privacy exemption to the Freedom of Information Act*, 9 J. Legal Studies 731 (1980).
[168] An Act to amend the Federal Deposit Insurance Act, to require insured banks to maintain certain records, to require that certain transactions in United States currency be reported to the Department of the Treasury, and for other purposes – Pub. Law 91-508, 84 Stat. 1114 - October 26, 1970 - 15 U.S.C. § 1681 et seq. The Act was an amendment to title VI to the *Consumer Credit Protection Act*, Pub. Law. 90-321, 82 Stat. 146 - June 29, 1968. The Act was passed together with the *Bank Secrecy Act* of 1970 (Pub. Law 91-508, 84 Stat. 1114 – 12 U.S.C, 15 U.S.C., 18 U.S.C. and 31 U.S.C.), which required banks and other financial institutions to keep certain records and report some transactions; financial institutions had to report deposits, withdrawals, currency exchanges or other payments exceeding 10.000$. Cf. SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 76 ff. for the two Acts.
[169] Cf. § 602(a)(4) [15 U.S.C. § 1681].

consumer reports can be done only if it is clearly and precisely disclosed to the consumer that this kind of report could be made[170].

Again with reference to financial information, in 1978 Congress adopted the *Right to Financial Privacy Act*[171]. The Act requires a subpoena or a search warrant for law enforcement for government officials who want to obtain financial records on an individual. Furthermore, when government seeks financial records, a notice to the individual is required before the disclosure of the information, so that the individual can challenge the release. This protection is provided only to individuals or small partnerships[172].

Two years later the *Privacy Protection Act* was passed[173]. Despite its name, the Act was not really connected to privacy in its more narrow meaning; rather, it ruled on First Amendment matters. In fact, the Act imposes restrictions on the search and seizure of product materials which reasonably were made as a form of public communication. Also in this case, officials must require a subpoena to obtain such information in order to enforce the law.

More directly related to electronic communication statutes are the *Cable Communications Policy Act of 1984*[174], on privacy protection for records held by cable companies, and the *Computer Matching and Privacy Protection Act of 1988*[175],that regulates the use of computer files in the investigations of governmental agencies. There are also many other acts on privacy, for example, regarding unsolicited phone

[170] An "investigative consumer report" is a "consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information" – cf. § 603(e) [15 U.S.C. § 1681a]. For more information on the *Fair Credit Reporting Act* see SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 361 ff.; SOLOVE, ROTENBERG, *Information privacy law*, cit., 519 ff.

[171] Pub Law 95-630, 92 Stat. 3697 – November 10, 1978 – 12 U.S.C. § 3401-3422. The Act was enacted partly as a response to the case *United States v. Miller*, 425 U.S. 435 (1976), cf. SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 71. In the cited case the Supreme Court held that a bank customer had no reasonable expectation of privacy in transaction records held by her bank. In the Court's view, the bank had control of that personal information and could handle and hold the data, thanks to the existence of a Federal statute that compelled the retention.

[172] Cf. SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 89 ff.

[173] Pub. Law. 96-440, 94 Stat. 1879, 42 U.S.C. § 2000aa et seq.

[174] An Act To amend the Communications Act of 1934 to provide a national policy regarding cable television Pub. Law No. 98-549, 98 Stat. 2780 - October 31, 1984.

[175] The Act amended the Privacy Act of 1974; cf. 5 U.S.C. §552a - Pub. Law. 100-503, 102 Stat. 2507 – June 16, 1989. The Act was a response to government matching of its employee records with records of individual enjoying federal benefits, in an attempt to catch people engaged in a fraud, cf. P. REGAN, *Legislating Privacy*, Chapel Hill (NC), 1995, 95 ff..

calls by telemarketers[176], unsolicited e-mails[177], and statutes which protect drivers'[178] or children's privacy[179].

Another statute, which is particularly interesting for this work, is the *Electronic Communications Privacy Act* of 1986 that updated federal electronic surveillance in order to keep up with new technologies[180]. The Act broadened the already existing protection for communications to include all forms of electronic transmissions. In particular, it is divided into three parts: the *Wiretap Act*, the *Stored Communications Act* and the *Pen Register Act*[181]. The Act classifies communications into three types: wire, oral and electronic communication. The Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include (A) any wire or oral communication […]"[182]. Electronic communications are, therefore, all communications that do not constitute wire or oral communications. An example is an email[183]. Communications

[176] *Telephone Consumer Protection Act* of 1991, to amend the Communications Act of 1934 to prohibit certain practices involving the use of telephone equipment. Pub. Law 120-243 - 47 U.S.C. § 227.

[177] It is usually known as SPAM. The Act is the *CAN-SPAM Act* of 2003 to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet – Pub. Law No. 108, 187- 117 Stat. 2699 - 15 U.S.C. 7701, et seq. – December 16, 2003.

[178] *Driver's Privacy Protection Act* of 1994, to amend title 18, United States Code, to protect the personal privacy and safety of licensed drivers, taking into account the legitimate needs of government and business - Pub. Law. 103-322, 18 U.S.C. §§ 2721-2725 - October 26, 1993. The Act restricts the states from disclosing or selling personal information recorded in their motor vehicle records.

[179] Children's Online Privacy Protection Act of 1998 - Pub. Law 105-277, 112, Stat. 2581-72815 - U.S.C. §§ 6501–6506, October 21, 1998. The Act restricts the possible uses of information gathered from children under the age of 13 by Internet websites.

[180] An Act To amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes - 18 U.S.C. § 2510-22 – Pub. Law No. 99-508, 100 Stat. 1848 – October 21, 1986.

[181] The Wiretap Act is codified at Title I of the *Electronic Communications Privacy Act*, 18 U.S.C. §§2510-2522 and governs the interceptions of communications. The *Stored Communications Act* can be found at 18 U.S.C. §§ 2701-2711. The Pen Register Act is at 18 U.S.C. §§ 3121-3127 and concerns pen registers and trap and trace devices, as well as more modern analogous devices. According to § 3127(3) a "pen register" is 'a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication […]".

[182] 18 U.S.C. § 2510(12).

[183] SOLOVE, ROTENBERG, *Information privacy law*, cit., 330; SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 142.

in transmission are covered and protected by the *Wiretap Act*, while the *Stored Communications Act* protects communications in storage.

In the internet environment, the information of communications and subscribers is stored by the electronic service providers. Section 2702(a), *i.e.* the *Stored Communications Act*, forbids service providers to disclosure the contents of stored communications. There are a number of exceptions, including disclosure to law enforcement agencies under certain circumstances[184]. In particular, as for the access to and disclosure of subscribers' records, section 2703(c) provides that a governmental entity may require a provider to disclose records or other information pertaining to a subscriber or a customer only when the entity "(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; (B) obtains a court order for such disclosure under subsection (d) of this section; (C) has the consent of the subscriber or customer to such disclosure;[…] (E) seeks information under paragraph (2)". Paragraph (2) establishes that the providers shall disclose the following data to the entity: name, address, local and long distance telephone connection records, or records of session times and durations, length of service and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address. Furthermore, the governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

There have been cases concerning ISP records in which disclosure was required by governmental agencies. For example, in the case *United States v. Hambrick*[185], the Federal Court applied the reasonable expectation of privacy test on ISP records and concluded that no reasonable expectation of privacy was there. This conclusion was reached on the consideration that a person cannot have a legitimate

[184] 18 U.S.C. § 2702(b). The process government should follow in case it wanted to access stored information varies depending on the time of storage. For example if it wanted to access communications that have been stored for more than 180 days, it should provide prior notice to the subscriber and obtain and administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order. Cf. 18 U.S.C. § 2703.

[185] 55 F. Supp. 2d 504 (1999). The text of the statute was different at that time, but for the purposes of this brief account of the case this does not matter.

expectation of privacy in information she voluntarily gave to other parties[186]. Once a subscriber reveals her information to an ISP, she cannot then claim to have a Fourth Amendment privacy interest in the same information[187]. The same approach was taken in another case, related to IP addresses[188] and URLs[189]. Since email and internet users rely on third-party equipment in order to engage in communication, they "have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information... [It is] voluntarily turned over in order to direct the third party's servers"[190]. The Court also reasoned that this kind of addresses does not reveal any contents of communication, but only unprotected addressing information. This conclusion was reached comparing physical mail to email. The outside part of a physical mail is not covered by Fourth Amendment protection, since what it is written on the envelope is considered visible and therefore voluntarily transmitted to third parties. The "visible" part of emails, such as to/from addresses, should therefore be considered in the same way[191]. In the same decision, the Court also stated that URLs could be more problematic if analyzed through a constitutional lens. Indeed, in the Court's words, "[a] URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://www.nytimes.com, whereas a

[186] This is the so called "third party doctrine" developed by the Supreme Court in the case *Smith v. Maryland*, 442 U.S. 735 (1979), 742 ff.
[187] Cf. *United Stats v. Kennedy*, 81 F. Supp. 2d 1103 (D. Kan. 2000), 1110.
[188] An IP number is "a unique number that identifies the precise location of a particular node on the Internet. The address is a 32-bit number usually written in dotted decimal format, i.e. in the form '123.33.22.32', and it is used by the TCP/IP protocol", see *Entry: Internet Address*, COLLIN, *Dictionary of Computing*, cit.
[189] URL is an abbreviation for Uniform Resource Locator" or "Universal Resource Locator". It is the address system used on the Internet, for example, to specify the location of documents in the World Wide Web. See *Entry: URL*, J. DAINTITH, E. WRIGHT (eds.), *A Dictionary of Computing*, Oxford, 2008.
[190] *United States v. Forrester*, 512 F. 3d 500 (9th Circ. 2008), 510.
[191] *United States v. Forrester*, cit., 510-511. See SOLOVE, SCHWARTZ, *Privacy, Information, and Technology*, cit., 184-185.

technique that captures URLs would also divulge the particular articles the person viewed"[192].

A very controversial piece of legislation is the *USA PATRIOT Act*. The Act, which was enacted right after the terrorist attacks of September 11, 2001, contains some provisions that affect individual privacy. With the aim of combatting terrorism, the *PATRIOT Act* tried to create a network of electronic crimes task forces which require information sharing among federal agencies. Furthermore, it mandated a new information system that allowed the State Department access to some criminal files kept by the FBI. There is also a provision which allows government investigator to search into educational records, without a court order[193].

Another critique which has often been made to the privacy protection regime of the USA is the necessity for individuals to "opt out" from the gathering of their information. More precisely, unlike what happens in the European and Canadian systems, in the USA whenever a consumer buys a product, her information is automatically processed by the selling company. The default rule allows the data holder to keep the data, with broad discretion in handling it. Whenever the consumer wanted to cease this processing of her data, she should *opt out*[194].

An interesting point to stress is that, despite the idea that seminal article by Warren and Brandeis pertained to the invasion of privacy by private entities (such as newspapers practicing yellow journalism), privacy regulation in the USA has acquired a different taste over time. In fact, as can be easily inferred from what has been said so far, in the US system, privacy is very often a way to escape

[192] *United States v. Forrester*, cit., 510 fn. 6.
[193] Cf. SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 141-143 and 101 ff.
[194] Only few people do indeed opt-out; see SOMA, RYNERSON, *Privacy Law, Privacy Law in a Nutshell*, cit., 180. It has been argued that the time and cost necessary for understanding how to opt out are so high that no consumer will ever engage in such activity. From an economic point of view, it seems that an opting-out system generates much more transaction costs than an opting-in system does (and that businesses can even have an interest in maintaining the transaction costs of opt-out higher). The latter would therefore be a better approach since it should increase the possibility that consumers choose according to their preferences. Cf. SOVERN, *Opting in, opting out, or no options at all: the fight for control of personal information*, cit., 1081 ff. As always happens, however, opinions can be divergent. For example, other scholars have claimed that an opt-in system would be more costly than an opt-out one, since the former would restrict the free flow of information which is vital for the current economic activities. This would in turn need companies to take steps in order to obtain the consent of consumers, to contact them individually for their "opting-in". This further step would make an opt-in system much more expensive than an opt-out one, which infers the permission of consumers when they do not explicitly object. Cf. M.E. STATEN, F.H. CATE, *The impact of opt-in privacy rules on retail credit markets: a case study of MBNA*, 52 Duke L.J. 745 (2003), 765-766.

governmental intrusion in one's private life. This has been explained in different ways: one can be found in Westin's famous book. The author claimed that this approach was a sort of reaction to the "over-surveilled" European society, from which part of the later American society came[195].

Another peculiarity is that in the US privacy is frequently coupled with anonymity, as both are included under First Amendment protection. This is becoming more and more common with regard to the internet world[196]. Many users believe that their activity on the web is anonymous and their identity is not known unless they choose to reveal it. As many lawsuits have demonstrated, this is not the case. Traces are left behind every time one uses the web, and users are identifiable in many ways such as, for example, the above-mentioned IP addresses. Indeed, ISPs have information which link IP addresses and other parameters to "real identities". As it will be shown with the support of some recent cases, the security of this information is strictly connected to the policies and carefulness of ISPs. In the last few years, a lot of civil lawsuits have been filed against "John Doe" defendants by plaintiffs who claimed they have been harmed in the Internet environment[197]. As we will see, decisions have taken different directions, even if the issue at stake was always the same.

2.3 Cases and solutions

2.3.1 Once upon a time in America

Once upon a time in America, in deciding the so-called "Sony Betamax" case[198], the Supreme Court ruled that "time shifting" constituted fair use and, therefore, there was no copyright infringement.

This seems a very old story, which has nothing to do with the other stories that will be told in this work. Actually, Sony Betamax is one of the most interesting and

[195] WESTIN, *Privacy and Freedom*, cit., 330.

[196] SOLOVE, SCHWARTZ, *Information privacy law*, cit., 554.

[197] "John Doe" is a fictional name given to a male party of a process, when his real name is not known or must remain withheld for legal reasons, see *Entry: John Doe*, BLACK, *Black's Law Dictionary*, cit., 750. The female corresponding is "Jane Doe".

[198] *Sony Corp. of America v. Universal City Studios, 464 U.S. 417* (1984) [*Sony Betamax Supreme Court*]. J. LITMAN, *The story of Sony v. Universal Studios: Mary Poppins Meets the Boston Strangler (Copyright)*, in J.C. GINSBURG, R.C. DREYFUSS, *Intellectual Property Stories*, New York, 2006, 358.

important cases where copyright collides (also) with users' rights. Leaving aside the importance of the first potential application of contributory and vicarious liability in copyright infringement, which lies at the foundation of the history of copyright enforcement against file sharing, and what usually remains untold is that in this suit some privacy concerns were also raised. It is for this reason that the history of Sony Betamax will be summarized in this context[199].

Sony was sued for contributory infringement of copyright laws for manufacturing and selling the Betamax, a video-recorder which could be used by individuals to record television programs on video tapes, in order to watch them at a more convenient time, a practice known as "time-shifting". The plaintiffs were Universal City Studios and Walt Disney, producers and copyright owners of many television programs and popular shows airing at the time Betamax was released.

In their opinion, since consumers used Betamax to record copyrighted works, defendants were liable for copyright infringement, under the US Copyright Act. Indeed, the lawsuit was focused on vicarious liability and contributory infringement. According to these doctrines, each of whose origins is in tort, a person may be held liable as an infringer for the infringement of someone else, even if not directly involved. Hence the first requirement of both these doctrines is the existence of a direct infringement. Courts have held that the rationale for secondary liability is that a party who distributes infringement-enabling products or services may facilitate direct infringement on a massive scale, in this way making it impossible for copyright owners to enforce effectively their rights. Therefore, the only alternative is to sue the distributor of the copying device[200].

Vicarious liability, whose origins are in the context of employment, refers to cases in which there is a special relationship between the infringer and the person being sued. This theory derives from the "*respondeat superior*" principle, by which an employer can be held liable for the infringing acts of an employee, when the latter is acting within the scope of employment. The application of this reasoning in the field of intellectual property infringement is much broader. Given the existence of a

[199] For the impact of the Sony Betamax Supreme Court decision, see LITMAN, *The story of Sony v. Universal Studios*, cit., 382 ff. and specially 386 ff. for the influence this case had on peer-to-peer litigation.
[200] *Arista Records, LLC v. Lime Group, LLC*, 715 F. Supp. 2d 481 (2010), 506.

direct infringement, vicarious liability is imposed when the following conditions exist: 1) the person has the power to supervise or control the infringer; and 2) she receives a financial benefit related to the infringer's activity. It does not matter whether the "superior" has or does not have knowledge of the infringing behavior[201].

Contributory infringement refers to someone who provides the way or the means for another person to violate copyright. "[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a "contributory" infringer"[202]. In this case the fundamental requirements are the nature of the infringing conduct, the person's awareness of the consequences of the infringement and if and how that conduct would be otherwise permissible[203].

The claim of the plaintiffs in *Sony Betamax* was clearly based on these doctrines. The production and distribution of the Betamax device was argued to have made Sony liable for the infringement perpetrated by end users. To prove the infringement and to obtain judgment against Sony, Universal sued also Mr. William Griffiths, a Sony customer who had bought a Betamax, "to be a nominal individual defendant"[204]. With regard to the distribution of the Betamax, Universal also sued certain retail stores which sold Sony's device, as well as the advertising agency that promoted it.

The District Court held in favor of Sony[205]. Judge Ferguson acknowledged that the crucial point of the suit was to understand whether "the individual and the retail defendants in recording plaintiffs' copyrighted works off-the-air [was] copyright infringement"[206]. The analysis started with the legislative history. The House Report accompanying the 1971 Amendment to the *Old Copyright Act* of 1909, related to sound recording piracy, touched upon the issue of home recording: "it is

[201] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 162.
[202] *Gershwin Publishing v. Columbia Artists Management*, 443 F.2d 1159, 1162 (2nd Cir. 1971).
[203] HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 163.
[204] LITMAN, *The story of Sony v. Universal Studios*, cit., 360.
[205] *Universal City Studios, Inc.* v. *Sony Corp. of America,* 480 F. Supp. 429 (C.D. Cal. 1979) [*Sony Betamax District Court*].
[206] *Sony Betamax District Court*, 441. Since some of these recording had been made earlier than 1976 Copyright Act came into force, the court had to analyze both the Old Act (1909) and the New Act (1976).

not the intention of the Committee to restrain the home recording, from broadcasts or from tapes or records, of recorded performances, where the home recording is for private use and with no purpose of reproducing or otherwise capitalizing commercially on it"[207]. At this point there was a sort of contrast between the just-quoted statement and the 1976 Act, since the latter appeared to grant copyright holders exclusive rights over *all* recordings. Judge Ferguson considered that the reasoning behind 1971 Amendment was incorporated into the Act of 1976, because "the language of the 1971 Amendment was incorporated into the New Act without any suggestion that legislative intent had changed"[208]. In support of its understanding of 1976 Act, the Court referred also the proceedings of the Conference Committee for the last mentioned Copyright Act. Judge Ferguson then proceeded to examine another possibility: home recording as a "fair use".

Fair use doctrine had been developed by courts and subsequently codified in 1976 Copyright Act[209]. It has been effectively defined as a "privilege in persons other than the owner of a copyright to use the copyrighted material in a reasonable manner without his consent, notwithstanding the monopoly granted to the owner"[210]. Taking into consideration all the factors required by section 107[211], the District Court found "that the home-use copying made possible by this new technology constitute[d] fair use of plaintiffs' works. The use, limited to home recording and

[207] *Sony Betamax District Court*, 444.
[208] *Sony Betamax District Court*, 444.
[209] According to HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 117 and MERGES ET AL., *Intellectual Property in the New Technological Age*, cit., 592, this concept originated in *Folsom v. Marsh*, 9 F. Cas. 342 (C.C.D. Mass. 1841). "Fair use" doctrine has been famously called "the most troublesome in the whole law of copyright" [see *Dellar v. Samuel Goldwyn, Inc*., 104 F.2d 661, 662 (2d Cir. 1939)]. Indeed, scholars and judges have been deeply reasoning on this tricky concept, born in common law and then codified in Copyright Act under § 107 of U.S.C. 17. It has been defined as an "equitable rule of reason" (*Sony Betamax Supreme Court,* 448), which means that every single case has it specific facts to be considered: this requires court to balance a variety of factors. Section 107 provides in fact a non-exhaustive list of factors that a court should consider [these factors are very closed to those Justice Story used in *Folsom v. Marsh*, 9 F. Cas. 342, 348 ff. (C.C.D. Mass. 1841)]. For a general overview of the fair use doctrine see HALPERN ET AL., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, cit., 116 ff.; HALPERN, *Copyright Law: Protection of Original Expression*, cit., 540 ff.; R.P. MERGES, J.G. GINSBURG, *Foundations of Intellectual Property*, New York, 2004, 387 ff. (gathering some of the most interesting scholars' contributions on the issue of fair use). For a deeper and more detailed analysis: L.E. SELTZER, *Exemptions and fair use in copyright: the exclusive rights tensions in the 1976 Copyright act*, Cambridge, 1978 and W.F. PATRY, *The fair use privilege in copyright law*, Washington, 1995.
[210] BALL H.G., *Law of Copyright and Literary Property*, New York, 1944, 260
[211] *Sony Betamax District Court*, 450 ff.

playback of audiovisual material broadcast free of charge to Betamax owners over public airwaves, [was] noncommercial and [did] not reduce the market for plaintiffs' works"[212].

As far as direct, contributory and vicarious liability concerned, Judge Ferguson immediately rejected the hypothesis of a direct infringement for the corporate defendants. With regard to contributory infringement, the District Court found that *a)* defendants did not have knowledge of the infringing activity (or if they had it, it was nonetheless insufficient); *b)* they did not induce or materially contributed to the infringement[213]; *c)* the Betamax was capable of "substantial" non-infringing use and that "[c]ommerce would […] be hampered if manufacturers of staple items were held liable as contributory infringers whenever they "constructively" knew that some purchasers on some occasions would use their product for a purpose which a court later deemed, as a matter of first impression, to be an infringement"[214]. Following this logic, the defendants were not held liable for vicarious liability either. Judge Ferguson argued that the application of this doctrine as made by plaintiffs went outside its scope[215].

In its reasoning, the District Court made a remark which is really interesting with regard to the core of this work. Ferguson J recognized that taking copyright enforcement further would mean entering into people's houses. Private behavior, such as home-recording, would be very difficult to control. In the legislative process leading up to the 1976 revisions to the Copyright Act, indeed, the Copyright Office was concerned "about invasion of the individual's privacy in his home". At the same time the District Court understood that "[o]f course, not all activity is made legal by virtue of occurring in a private home. Congress can constitutionally legislate against some activity which may occur in the home, but doing so necessarily requires caution. Here, legislative history shows that, in balance, Congress did not find that protection of copyright holders' rights over reproduction of their works was worth the privacy and enforcement problems which restraint of home-use recording would create" [216]. So, according to Judge Ferguson, in this case it was Congress who had

[212] *Sony Betamax District Court*, 456.
[213] *Sony Betamax District Court*, 459-460.
[214] *Sony Betamax District Court*, 461.
[215] *Sony Betamax District Court*, 461 ff.
[216] *Sony Betamax District Court*, 445-446 *passim*.

struck the balance between consumers' privacy and copyright enforcement. More recently, this heavy task appears to have been shifted on Courts, which have a hard time coping with it, as it has been and will be demonstrated throughout this work.

Universal appealed to the Ninth Circuit Court of Appeals.[217]. The panel analyzed the fair use requirements listed in section 107 and found that home-recording was not fair use, since:

a) the use, despite not commercial, was not "for convenience" and could not qualify as fair;

b) the nature of the copyrighted material, which was entertainment work, played against fair use qualification in the second factor, since fair use is broader when informational types are concerned;

c) the reproduction of the work consisted in a whole reproduction and was not confined to a portion;

d) there was a negative effect of the use upon the potential marked of the copyrighted work[218].

The Ninth Circuit found that videotape recorders were manufactured, advertised and sold for primary purpose: reproducing television programming. Since virtually all television programs are copyrighted, then the recorders where not saved by the doctrine of substantial noninfringing use[219]. According to the panel of judges, the lower court's staple article of commerce theory was "inappropriate"[220]. Finally, regarding to contributory and vicarious liability, the Court held that it was not necessary that the defendants had actual knowledge of the infringing activity. Their "innocence" would not shelter them from liability; rather it would only affect the remedies available. Sony knew that Betamax would be used to reproduce copyrighted works; they expected that the device would be used mostly for recording programs off-the-air. The Court held that also the other requirements were met, since

[217] *Universal City Studios, Inc.* v. *Sony Corp. of America,* 659 F.2d 963 (9th Cir. 1981) [*Sony Betamax Ninth Circuit*]. For an Italian translation and a comment see G. PASCUZZI, *Videoregistrazione e "copyright" statunitense: violazione, "fair use" o terza via?*, in *Foro it*., 1984, IV, 23.

[218] *Sony Betamax Ninth Circuit*, 969 ff. *passim*.

[219] *Sony Betamax Ninth Circuit*, 975.

[220] *Sony Betamax Ninth Circuit*, 975.

the defendants had induced, caused or materially contributed to the infringing conduct of consumers. As such, they had to be held accountable[221].

Eventually the case arrived at the Supreme Court[222]. In a narrow 5-4 decision, the majority held that, despite the fact that copyright law did not expressly provide for contributory liability, it did not mean that it was not applicable. "For vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another"[223]. As far as vicarious liability was concerned, the Court reasoned that Sony could be held liable only for the fact that it sold the equipment with constructive knowledge of the fact that customers could use it to make unauthorized copies of copyrighted material. However, there were no similar precedents, except in patent law[224]. The Court applied the so-called "staple article of commerce doctrine", which is derived from patent law. In particular, the Patent Act[225] expressly provides that the sale of a staple article of commerce suitable of substantial non-infringing use does not constitute contributory infringement[226]. But when a device is adapted to an infringing use, as well as to other lawful uses, this is not enough to make the seller a contributory infringer. The mentioned doctrine must strike a balance between the copyright holder's legitimate demand for protection and the rights of the others to engage in unrelated areas of commerce. So, the U.S. Supreme Court held that the sale of copying equipment did not constitute copyright infringement, as long as the product could be widely used for "legitimate, unobjectionable purposes". The product only needed to be capable of substantial non-infringing uses[227]. According to Justice Stevens, who wrote the majority opinion, Sony had demonstrated the existence of these non-infringing uses: noncommercial time-shifting was one of

---

221 *Sony Betamax Ninth Circuit*, 975-976.

222 For an Italian translation and a commentary see G. PASCUZZI, *La videoregistrazione domestica di opere protette davanti alla "Supreme Court"*, in *Foro it*., 1984, IV, 351. For the complete interesting history of how the Supreme Court reached this 5-4 majority decision see LITMAN, *The story of Sony v. Universal Studios*, cit., 366 ff.

223 *Sony Betamax Supreme Court*, 435.

224 *Sony Betamax Supreme Court*, 439.

225 U.S. Patent Act, 35 U.S.C. § 1-376.

226 *Sony Betamax Supreme Court*, 440 referring to 35 U.S.C. § 271(c).

227 *Sony Betamax Supreme Court*, 440-442.

them. This use could indeed be considered as fair use[228], since time-shifting was a noncommercial and nonprofit activity. The fact that the entire work was reproduced did "not have its ordinary effect of militating against a finding of fair use": time-shifting merely enabled a person to watch the program. This use had no effect upon the potential marked for the copyrighted work. Inhibiting such activity would simply stop the access to ideas, without any valuable benefit. Furthermore, the' plaintiffs failed to demonstrate the likelihood of future economic harm coming from the use of Betamax[229]. In the end, since time-shifting was a species of fair use and there was no harm to the market for copyrighted work, Sony was not held liable for contributory infringement[230].

As it will be demonstrated in this work, the *Sony Betamax* decision is closely linked to peer-to-peer file sharing. In particular, what is really interesting is that enforcing copyright rights today triggers the same privacy concerns that were raised at that time[231].

2.3.2 The first steps of copyright holders against MP3 file sharing

The Recording Industry Association of America (RIAA) represents the interest of US recording industry and the holders of music copyright[232]. As soon as MP3 technology hit the market, the RIAA understood that free download of MP3 files could be a threat to its affiliates' business and, in turn, also to *its* business. Indeed, this kind of file compression format resulted in much smaller files than previous data formats[233].

---

228 *Sony Betamax Supreme Court*, 447 ff.

229 *Sony Betamax Supreme Court*, 450-451.

230 *Sony Betamax Supreme Court*, 456. The dissenting opinion by Justice Blackmun put its attention on the harm Betamax could cause to plaintiffs' market. "The videotape recorder deprived copyright owners of the opportunity to exploit the market of potential viewers who found it inconvenient to watch television programs at the time they are broadcast", see LITMAN, *The story of Sony v. Universal Studios*, cit., 382 on *Sony Betamax Supreme Court*, 457-493.

231 LITMAN, *The story of Sony v. Universal Studios*, cit., 386; see also J. LITMAN, *Copyright and Personal Copying: Sony v. Universal City Studios Twenty-One Years Later*, 55 Case W. Res. 917, spec. 953 ff. (2005).

232 "The Recording Industry Association of America (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", see RIAA's website: http://www.riaa.com/aboutus.php. According to MERGES ET AL., *Intellectual Property in the New Technological Age*, cit., 682, the RIAA represents more than 500 companies related to the creation, manufacturing, and distribution of sound recording.

233 MP3 – full name MPEG audio level 3 – is "a way of encoding digital audio data into a compressed data format that is approximately one twelfth the size of the original without perceptible

This enables users to store a bigger quantity of files and, most important, to exchange them more quickly and more easily than before.

The very first step that the RIAA took against this perceived threat was to try to stop the production and sale of the first MP3 player[234]. The RIAA asserted that the "Diamond Rio" MP3 reader did not meet the requirements for the AHRA[235], since it lacked a "Serial Copy Management System". This system would have verified the copyright status and generation of the files that it played[236]. To the RIAA's disappointment, the Court held that since the device could only make copies from a computer hard drive, it was not a digital audio recording device and therefore not within the ambit of the Act. Indeed, in Judges' opinion, "because computers are not digital audio recording devices, they are not required to comply with the Serial Copyright Management System requirement and thus need not send, receive, or act upon information regarding copyright and generation status"[237]. Furthermore, the Court applied the reasoning of the Supreme Court majority in *Sony Betamax*, analogizing the the "time-shifting" of the Betamax to the "space-shifting" (or, as is now more often said, the "format-shifting") of Diamond Rio[238]. Later on the two parties reached a settlement[239].

In 1999, the RIAA was the protagonist in a case against MP3board.com. MP3board.com developed a search engine that could trawl the internet for MP3 files and provide links to them. The RIAA wrote a letter to the site managers and asked for a halt to the operation of the service. MP3board.com filed an action in June 2000 seeking a declaration that hypertext linking created by automated processes was not a copyright infringement, even if the destination of a link is to a website containing

---

loss of quality.[…]. Because MP3 files are compact and easy to copy, they are relatively quick to download and very easy to distribute -which is causing problems for the original artists who are trying to protect their copyright material", *Entry: MP3*, S.M.H. COLLIN, *Dictionary of Computing*, cit.

[234] *RIAA v. Diamond Multimedia System, Inc.,* 29 F. Supp. 2d 624 (C.D. Cal. 1998) and *RIAA v. Diamond Multimedia System, Inc*., 180 F.3d 1072 (9th Cir. 1999) [*Diamond Rio II*]. For a comment see T.J. BARTHEL, RIAA v. Diamond Multimedia System, Inc.: *The Sale of The Rio Player Forces The Music Industry to Dance to a New Beat*, 9 DePaul-LCA J. Art & Ent. L. 279 (1999); E.R. GOSSE, Recording Industry Association of America v. Diamond Multimedia System, Inc.: *The RIAA could not stop the Rio-MP3 Files and the Audio Home Recording Act*, 34 U.S.F. L. Rev. 575 (1999).

[235] 17 U.S.C.S. § 1001 et seq.

[236] *Diamond Rio II*, 1075.

[237] *Diamond Rio II*, 1078.

[238] *Diamond Rio II*, 1079: "The Rio merely makes copies in order to render portable, or "space-shift," those files that already reside on a user's hard drive".

[239] GOSSE, Recording Industry Association of America v. Diamond Multimedia System, Inc.: *The RIAA could not stop the Rio-MP3 Files and the Audio Home Recording Act*, cit., 597.

infringing material. The District Court denied the motions for summary judgment of both parties, claiming that the legality was related to the proof of the defendant's knowledge of infringement. After years of litigation, the parties eventually settled the dispute and MP3board.com dropped its MP3 search engine[240].

In 2000, another web portal (MP3.com) developed a successful service (MyMP3.com), that enabled subscribers to develop a virtual online music locker with a password, through which they could access music files copied and stored on MP3.com's servers from any computer connected to the Internet. The system was based on the idea of "space shifting"[241], already applied in the case of Diamond Rio. The major record labels sued MP3.com claiming that its initial copying of CDs onto its server and the distribution of the same to the subscribers infringed their copyright. The trial court rejected the fair use defense of MP3.com[242], which later settled the case[243].

A further step by RIAA was to confront file-sharing systems. File sharing is a system of distributing electronic information, as for example music or video files, through a network. In particular, in a peer-to-peer (P2P) file sharing system participants have all the same privileges; that is the reason why participant users are called "peers". Each peer acts simultaneously as a client and as a server. These systems can be either centralized, when there is a central server, or decentralized, when such a server does not exist and all computers act as clients and servers (this latter is a pure P2P system)[244].

An example of a centralized P2P system was Napster, the world's first effective peer-to-peer file sharing service. Napster concentrated on MP3s music files: end users could download from the Internet a software, which enabled them to share hundreds of thousands songs among each other. In 2000, Napster was sued by eighteen recording companies for contributory and vicarious copyright infringement.

---

[240] *Arista Records, Inc., et Al., v. MP3Board, Inc.*, 2002 U.S. Dist. LEXIS 16165.

[241] MERGES ET AL., *Intellectual Property in the New Technological Age*, cit., 683.

[242] See *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

[243] MP3.com first settled with four of the five record labels; later, when the court assessed liability to Universal Music Group (UMG), MP3.com settled also with the fifth label, cf. MERGES ET AL., *Intellectual Property in the New Technological Age*, cit., 684 and M. GEIST, *Internet Law in Canada*, Concord, 2002, 521 ff.

[244] R. STEINMETZ, K. WEHRLE, *Peer-to-peer systems and applications*, Berlin - New York, 2005, 10 ff. The authors explain that P2P is not just a technology for file-sharing; rather, it is a "fundamental design principle for distributed systems". For a brief history of P2P file sharing softwares see *Ibidem*, 18 ff.

The companies sought first of all to enjoin Napster's activity of assisting others in copying plaintiff's copyrighted works without permission[245]. Napster based it defenses on fair use, substantial non-infringing uses[246] and DMCA safe harbors[247]. Napster was not involved in ripping the audio CDs in users' computers, nor did it store files on its system. The District Court found that, unlike the case of "time-shifting" in *Sony Betamax*, Napster facilitated the distribution of infringing MP3. Furthermore, Napster continuously controlled users' access and did not just manufacture and sell a product. For these reasons, the Court held that Napster could not enjoy the fair use harbor[248] and that it encouraged and assisted users in the act of infringement. Napster also facilitated the exchange of files stored in users' hard disks. Indeed it created a library on each of the users' computer and permitted the search for MP3 files located in other users' PCs. Furthermore, it enabled the direct transfer of MP3s from user to user (peer-to-peer). Referring to these arguments, the District Court held Napster liable for vicarious infringement. As a consequence, Judge Patel enjoined Napster "from engaging in, or facilitating others in copying, downloading, uploading, transmitting or distributing plaintiffs' copyrighted musical compositions and sound recordings, protected by either federal or state law, without express permission of rights owner"[249].

On appeal by Napster, the Ninth Circuit affirmed the ruling[250]. The decision was based on the district court's findings, and this even if the Court of Appeals recognized that Napster did also have some non-infringing uses, such as the distribution by artists of their music. The Court found that Napster was aware of the direct infringement and that this limited the applicability of the "Betamax doctrine"[251]. Napster had also the right and ability to control users' activity and

---

[245] *A&M Records, Inc., v. Napster*, 114 F. Supp. 2d 896, 900 (N.D. Cal. 2000) [*Napster District Court*], see R.P. BEETS, *RIAA v. Napster: The Struggle to Protect Copyrights in the Internet Age*, 18 Ga. St. U. L. Rev. 507 (2001); T.J. RYAN, *Infringement.com:* RIAA v. Napster *and the Was Against Online Music Piracy*, 44 Ariz. L. Rev. 495 (2002). The case of Napster had a worldwide eco, see for example: G. PASCUZZI, *Opera musicali su Internet: il formato MP3*, in *Foro it*., 2001, IV, 101; P. AUTIERI, *Il caso Napster alla luce del diritto comunitario*, in L.C. UBERTAZZI (ed.), *TV, Internet e «new trends» di diritti d'autore e connessi*, Milano, 2002, 63.

[246] Also called "Betamax doctrine" following *Sony Betamax Supreme Court* decision.

[247] 17 U.S.C. § 512, see *infra*.

[248] *Napster District Court*, 913 ff.

[249] *Napster District Court*, 927.

[250] *A&M Record Inc. v. Napster, Inc.*, 239 F.3d 1004 (2001) [*Napster Appeal*].

[251] *Napster Appeal*, 1014-1015.

"knowingly encourage[d] and assist[ed] the infringement of copyrights"[252]. Without Napster's support services, users could not find and download music, which meant that Napster contributed to the infringement[253]. As far as vicarious liability was concerned, despite the ability to effectively control users, Napster could obtain a profit only by failing to stop users' infringing behavior. In fact, the more users registered, the more music was available, which in turn meant more users and so on. More precisely, the more potentially infringing material was available, the more users were likely to be attracted and the more profitable would be the venture. This meant that there was a financial benefit for Napster that was directly linked to the infringement of copyright[254]. Vicarious liability requirements were thus met. Napster was later shut down, following an injunction granted to A&M Records[255].

The music industry won this initial legal battle against P2P technologies; but technology was fighting back hard. After Napster's disappearance, new networks appeared. Successors to Napster in the first instance were Aimster[256] and AudioGalaxy. These were in turn supplanted by Morpheus and KaZaA, which were in turn overtaken by eDonkey and Bit Torrent[257]. As can easily be imagined, after the victory against Naspter, the recording industry sued other P2P software companies. The ensuing suit against Grokster became one of the most seminal cases in US copyright law, second perhaps only to *Sony Betamax*[258].

---

[252] *Napster Appeal*, 1020.
[253] *Napster Appeal*, 1022, quoting *Napster I*, 919-920.
[254] *Napster Appeal*, 1023 ff.
[255] A&M Records, Inc. v. Napster, Inc., 2001 U.S. Dist. LEXIS 2186 (N.D. Cal., 2001). Later on, due to the suits which was subject, Napster eventually went bankrupt; in 2008 was bought by a bigger company.
[256] Aimster was sued by RIAA right after the RIAA won against Napster. RIAA won also this battle: *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003), *cert. denied* 540 U.S. 1107 (2004).
[257] See J. BORLAND, *Peer to peer: As the revolution recedes*, CNET News.com, December 31, 2001 available at: http://news.cnet.com/2100-1023-277478.html; J. BORLAND, *P2P users traveling by eDonkey*, CNET News.com, August 28, 2005, available at: http://news.cnet.com/P2P-users-traveling-by-eDonkey/2100-1025_3-5843859.html. "BitTorrent is a way to transfer files of just about any size quickly and efficiently. It works by breaking files up into small pieces. The file is downloaded piece by piece from one or many different sources. It's efficient because you get faster downloads using a lot less bandwidth. The name BitTorrent is also used to describe the official BitTorrent client. […] Since the file is broken up into small pieces, little bandwidth is used to do the overall transfer. Once the file is finished downloading, the client software continues to share the completed file (becoming a "seed") with others looking for it. This also means the file can still be downloaded long after the original poster has stopped seeding the file", cf. http://www.bittorrent.com/help/faq/concepts, "*What is BitTorrent?*".
[258] *MGM Studios, Inc., v. Grokster, Ltd*, 259 F.Supp. 2d 1029 (C.D. Cal. 2003) [*Grokster District Court*]; *MGM Studios, Inc., v. Grokster, Ltd*, 380 F.3d 1154 (9th Cir. 2004) [*Grokster Appeal*]; *MGM Studios, Inc., v. Grokster, Ltd*, 545 U.S. 913 (2005) [*Grokster Supreme Court*], see D.R. LEVIN, *The*

The plaintiffs in *Grokster* were the usual "organizations in the motion picture and music recording industries" and defendants, Grokster, a P2P service that "distributed software that enabled users to exchange digital media via a peer-to-peer transfer network"[259]. Grokster distributed software which could be downloaded for free. Through this software users could share files located on their own computers. The software automatically connected to a P2P network and made files available for transfer to other users connected to the network. Grokster also provided some means through which a user might search the shared files[260]. Thus, the plaintiffs contended that Grokster's conduct rendered it liable based on contributory and vicarious liability.In order to demonstrate Grokster's liability, MGM had to prove the direct infringement of users. Citing *Napster*, the District Court held that it was "undisputed the at least some of the individuals who use defendants' software [were] engaged in copyright infringement of plaintiffs' copyrighted works"[261]. Thus, they infringed plaintiffs' rights of reproduction and distribution. The Court first analyzed the allegedly contributory infringement. As already stated, liability for contributory infringement requires two factors to be taken into account: 1) "knowledge of" and 2) "material contribution to" the infringing conduct of another. In light of *Sony Betamax*, the Ninth Circuit in *Napster* refused to ascribe liability to Napster, simply because it knew that P2P technology could be used for infringing activity. Instead actual knowledge of the infringement and the failure of acting despite knowing were required[262]. Since Grokster marketed itself as "the next Napster", it clearly knew that most of the individuals who downloaded its software used it to infringe copyright. The question was about the actual knowledge of Grokster and its failure of potentially acting to prevent infringement[263]. Then came the question of the material contribution in users' infringement. In *Napster*, both the District Court and the Appeals Court held that without the support services of Napster, users could not find and download music. When Napster shut down its servers, the network disappeared

Future of Copyright Infringement: Metro-Goldwyn-Mayer Studios, Inc., v. Grokster, Ltd., 21 St. John's J. Legal Comment. 271(2006). For an interesting parallelism between *Sony Betamax* and *Grokster*, see LITMAN, *The story of Sony v. Universal Studios*, cit., 387 ff.

259 *Grokster District Court*, 1032. Even if plaintiff were more than one, we will refer only to MGM; the same will be made with defendants, collectively referred as Grokster.

260 *Grokster District Court*, 1032.

261 *Grokster District Court*, 1034 referring to *Napster Appeal*, 1013-1014.

262 See *Napster Appeal*, 1021.

263 *Grokster District Court*, 1037-1038.

and its customers could not exchange file anymore. In this case, differently from Napster, Grokster did not operate a centralized file-sharing network[264]. Napster utilized a "supernode" owned and operated by the same company. Grokster did not: users did not need to transmit information to or through any computer owned or controlled by Grokster. Furthermore, Grokster did not provide any facility for direct infringement or was it in any way materially involved in infringement. Even if Grokster were to deactivate its computers, users would still be able to share files. Despite the fact that Grokster supplied some support services, there was no substantial contribution to the infringement[265].

With regard to vicarious liability, the Court listed the two elements needed: 1) a financial benefit and 2) the right and ability to supervise the infringing conduct. As already mentioned, as opposed to contributory infringement, in this case one can be held liable even without knowledge of infringement. Grokster clearly gained a financial benefit from the infringing conduct: despite thr fact that the software was distributed for free, the company did derive substantial revenues from advertising. Advertising was connected to the number of individuals who downloaded the software. Since many of them used Grokster for sharing copyrighted works, a significant proportion of defendant's revenues depended upon infringement[266]. However, Grokster had no ability to control what users did. As stated above, Napster had a central server and possessed the power to terminate users' account (which it actually did sometimes). In the case of Grokster, in contrast, the network was even property of another company[267].

Thus, the District Court found Grokster not liable.

MGM appealed to the same Ninth Circuit Court of Appeals that just a couple of years before had decided Napster's destiny.

The Ninth Circuit analyzed first the issue of contributory infringement, stating that "[i]f the product at issue [was] not capable of substantial or commercially significant non-infringing uses, then the copyright owner need[ed] only show that the defendant had constructive knowledge of the infringement. On the other hand, if the

[264] Previously Grokster applied a centralized-type network, as it appears from *Grokster District Court*, 1032 ff; see also *Grokster Appeal*, 1166.
[265] *Grokster District Court*, 1039-1043.
[266] *Grokster District Court*, 1043-1044.
[267] *Grokster District Court*, 1045-1046.

product at issue [*was*] capable of substantial or commercially significant non-infringing uses, then the copyright owner [had to] demonstrate that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement"[268].

Since the District Court had found that the software distributed by Grokster was capable of substantial non-infringing uses, it correctly applied the "reasonable knowledge" of specific infringement standard. Furthermore, the judges observed that contributory infringement required knowledge as well as material contribution. Grokster had a decentralized structure, so that even if it had closed its door, users could still have shared files. To the Court this meant no knowledge of what users did[269]. As for material contribution, the Ninth Circuit found that Grokster was not contributing, since it did not provide neither the site nor the facilities for infringement, nor did the files reside on its computers. And even if Grokster might seek to be "the next Napster"[270], its technology could be used for other numerous uses[271].

The Court then evaluated the possibility of vicarious liability. In considering Grokster's power and ability to supervise, the Ninth Circuit found that the sort of monitoring and supervisory relationship that was usually present in vicarious liability cases was totally absent in this instance. The relationship between Grokster and its users was, in judges' opinion, very different from the one occurring between Napster and its users[272]. For these reasons the Ninth Circuit affirmed the District Court's decision.

In the aftermath of these two decisions, major labels and other copyright holders started to realize that suing ISPs was not worthwhile anymore. The design of a decentralized P2P system had created an alibi for those companies producing the software, which had no longer had an active role in the exchange of files[273].

---

[268] *Grokster Appeal*, 1161 (emphasis in original).
[269] *Grokster Appeal*, 1161-1163.
[270] *Grokster District Court*, 1036.
[271] *Grokster Appeal*, 1164.
[272] *Grokster Appeal*, 1164-1166.
[273] DMCA as well as European Directive 2000/31/EC, introduced so called "safe harbors provisions" for Service Providers (see *infra*). Basically, when an ISP follows the behavior prescribed by the statute, it qualifies for a safe harbor and therefore its liability is limited. Even if European and American legislation are somehow different [see M. PEGUERA, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 Columbia Journal

Copyrighter holders had to think of a new way of enforcing their rights. Therefore, a new kind of lawsuit spread, in which copyright holders would try to sue end users for their infringing behaviors. These suits will be later analyzed in detail.

Nevertheless, MGM did successfully challenge the Ninth Circuit Court's decision in the US Supreme Court, where the justices unanimously reversed lower court decisions[274]. From the inception of the first lawsuit, direct infringement by users had never been questioned. The Supreme Court held that Grokster unmistakably knew that its users employed the software primarily to download copyrighted files. Indeed, from time to time, the company had learned about these infringements, since it had received emails from users pertaining copyrighted movies that they had downloaded. The Court's opinion was that Grokster was more than a merely passive recipient of information. The company had used an OpenNap system, which apparently was engineered to substitute Napster. Therefore, it seemed to the Court that Grokster wanted to capture the market of former Napster users. Grokster sent users a newsletter advertising its ability to provide some copyrighted materials. As said, the company earned money by selling advertising space: as the number of users increased, advertising opportunities increased as well. Despite the fact that Grokster occasionally sent emails to its users about infringing content, it never blocked anyone's access when it was noticed by content owners [275].

The main thrust of the Supreme Court's reasoning was to strike the balance between "supporting creative pursuits through copyright protection and promoting innovation in new communication technologies by limiting the incidence of liability for copyright infringement" [276]. The Court underlined that in this case imposing liability seemed mandatory, because of the high diffusion of infringing activities[277]. So the Supreme Court analyzed again the possibility of a contributory or a vicarious liability of Grokster. Justice Souter, delivering the opinion, wrote that contributory infringement can be carried out also by "inducing" or "encouraging" direct

---

of Law & the Arts 481, 2009] and even if in the case of Napster this act was not applied, this kind of statutes have sometimes protected Internet Providers from copyright holders' claims: see for example *Viacom Int'l, Inc. v. YouTube, Inc*., 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

[274] There were two concurring opinions: one from Justice Ginsburg, joined by the Chief Justice and Justice Kennedy (*Grokster Supreme Court*, 942 ff.) and one from Justice Breyer, joined by Justice Stevens and Justice O'Connor (*Grokster Supreme Court*, 949 ff.)

[275] *Grokster Supreme Court*, 923-927.

[276] *Grokster Supreme Court*, 928.

[277] *Grokster Supreme Court*, 929.

infringement[278]. So, while the Supreme Court decided not to revisit formally the *Sony Betamax* safe haven, it did proceed to correct the misapplication of the Ninth Circuit Court of Appeals[279].

In particular, the act of advertising an infringing use or of instructing how to engage in such a use showed an affirmative intent that the product be used for that scope. In the Court's view, this can make the distributor of a device liable for the infringement by third parties[280]. Three particular actions undertaken by Grokster guided the Court: 1) the company tried to satisfy the market built and later abandoned by Napster; 2) the company did not make any attempt to develop filtering tools or to diminish the infringing activity through other means; and 3) Grokster made money by selling advertising space, whose value grew as the volume of use grew[281].

Accordingly, the Supreme Court remanded the case for further proceedings consistent with its opinion, holding Grokster liable. With this decision on their side, recording companies started a new wave of suits against software distributors, in which the former regained an increasing measure of success[282].

2.3.3 Lawsuits against individual users

a) Before the Verizon cases

Beginning in the summer of 2003, the RIAA tried a new strategy to enforce the rights of its associates. They chose to sue persons with an internet access that the RIAA had reason to believe to be used for peer to peer file sharing[283].

The recording industry first concentrated on "uploaders": people sharing a folder on their personal computers (PC) that allowed others to copy music files. To detect whether there was an illegal sharing of recordings owned by its affiliates, the

---

[278] Souter J referred to *Gershwin Publishing v. Columbia Artists Management*, cit., 1162.
[279] *Grokster Supreme Court*, 933-934.
[280] *Grokster Supreme Court*, 935-937: "The inducement rule […] premises liability on purposeful, culpable expression and conduct".
[281] *Grokster Supreme Court*, 939-941.
[282] See later in this chapter.
[283] See R. BACKERMAN, *How the RIAA litigation process works*, 2008, available at: http://beckermanlegal.com/howriaa.htm. Actually RIAA had already sued in April 2003 four college students for developing and maintaining search engines that allowed the exchange of files among students in the campus; at that time RIAA's tactic caused a great stir, since the idea of suing students seemed an heavy-handed approach, see EFF, *RIAA v. The People: Four Years Later*, 2007, 3 at: http://w2.eff.org/IP/P2P/riaa_at_four.pdf.

RIAA's investigators ran the software on their own computers, exactly the same way as any other P2P user would do[284]. Then they searched for songs owned by their labels and collected the Internet Protocol (IP) addresses of the users who were offering those recordings. The RIAA could not match an IP address to a "real" identity without the intervention of an ISP. To reach this result, the Association applied for a special subpoena power provided by the Digital Millennium Copyright Act.

The strategy of the RIAA was as simple as it gets: fill out a subpoena request and give it to a federal clerk to obtain personal information on people the RIAA believed were pirating and sharing copyrighted songs. Once these names and addresses had been obtained, the RIAA could sue end users directly. In particular, the recording industry sought damages under the Digital Theft Deterrence and Copyright Damages Improvement Act of 1999[285], that allows copyright holders to sue infringers for damages ranging from $750 to $30,000.

As prescribed by section 512(h)(2) of the DMCA, the request for the subpoena shall be accompanied by "(A) a copy of a notification described in subsection (c)(3)(A); (B) a proposed subpoena; and (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under [the same] title". The process seems to rely on celerity: if the request submitted by the copyright owner satisfies some specific requirements, "the clerk shall *expeditiously* issue and sign the proposed subpoena and return it to the requester for delivery to the service provider"[286]. "Upon receipt of the issued subpoena, [...] the service provider shall *expeditiously* disclose to the copyright owner or person authorized by the copyright owner the information required by the

[284] See R. BACKERMAN, *Large Recording Companies v. the Defenseless – Some Common Sense Solution to the Challenges of the RIAA litigation*, 47 Judge J. 20, 20 (2008). Later on, RIAA used also another methodology: they put into P2P networks files with popular names of songs. But these files actually were corrupted, junk files (this technique is called "spoofing"), see KAO, *RIAA v. Verizon: Applying the Subpoena Provision of the DMCA*, cit., 425. See also: http://www.thepirateparty.com/index.php/references/34-external/70-how-it-does-it-the-riaa-explains-how-it-catches-alleged-music-pirates. Spoofing can be defined as "a method of gaining unauthorised access to a computer or network by pretending to be an authorised computer or device", see *Entry: IP spoofing*, COLLIN, *Dictionary of Computing*, cit.

[285] This Act emended 17 U.S.C. § 504(c).

[286] 17 U.S.C. § 512(h)(4), emphasis added.

subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification"[287].

Some ISPs complied with the requests of the RIAA, which subsequently sent letters to and filed lawsuits against hundreds of individuals. Verizon Online (Verizon)[288] was the first ISP to refuse to comply with the RIAA's subpoena and fought back against the RIAA.

b) RIAA v. Verizon

In July 2002, the RIAA served a subpoena on Verizon, seeking information to identify a person that seemed to be using the P2P software KaZaA for the illegal downloading of songs[289]. The subpoena included the user's internet IP address, to enable Verizon to locate the computer of the infringer, as well as the time and date the songs were downloaded. As requested by section 512(h)(2)(c), RIAA presented a sworn declaration that the information was sought in good faith and that would only be used to enforce the rights of its members[290]. The RIAA asked Verizon for immediate assistance to block the unauthorized activity of file sharing. The RIAA specifically asked that the ISP remove or disable access to the infringing sound files through it system[291].

Verizon answered with a letter in which it refused to comply with the RIAA's subpoena. As a response, the Recording Industry filed a motion to compel production. Verizon opposed the motion: according to Verizon's interpretation of DMCA, section 512(h) applied only if the infringing material is stored on the service

---

[287] 17 U.S.C. § 512(h)(5), emphasis added.

[288] "Verizon Communications Inc., headquartered in New York, is a leader in delivering broadband and other wireline and wireless communication innovations to mass market, business, government and wholesale customers", see http://investor.verizon.com/profile/index.aspx.

[289] *Verizon* cases have been widely analyzed and dozens of scholars' contributions have been written. For a general recap see: A. KAO, *RIAA v. Verizon: Applying the Subpoena Provision of the DMCA*, 19 Berkeley Tech. L.J. 405 (2004); D. GORSKI, *The Future of the Digital Millennium Copyright Act (DMCA) Subpoena Power on the Internet in Light of* Verizon Cases, 24 Rev. Litig. 149 (2005); T.A. DUTCHER, *A Discussion of the Mechanics of the DMCA Safe Harbor and Subpoena Power, as Applied in* RIAA v. Verizon Internet Services, 21 Santa Clara Computer & High Tech. L.J. 493 (2005); K. RAYNOLDS, *One Verizon, Two Verizon, Three Verizon, More? – A Comment: RIAA v. Verizon and How The DMCA Subpoena Power Became Powerless*, 23 Cardozo Arts & Ent. L.J. 343 (2005).

[290] *In re Verizon Internet Services*, 240 F. Supp. 2d 24 (D.D.C. 2003), 37, 28 [*Verizon I*]

[291] *RIAA v. Verizon Internet Services*, 351 F.3d 1229, 1233 (DC Cir. 2003) [*Verizon Appeal*].

provider's system or network under subsection 512(c)[292]. Since Verizon was acting simply for the transmission of information from user to user, there was no material stored on its system. Therefore, it argued, the subpoena could not be applied in its case.

Meanwhile the RIAA served a second subpoena on Verizon. The ISP opposed again and this time it also raised constitutional issues[293].

The RIAA got the better of Verizon in the trial level decisions and obtain rulings that forced Verizon to divulge users' identities[294]. In the opinion of the District Court for the District of Columbia, section 512(h) had to be applied to every kind of service provider. But the Court of Appeals reversed[295]. The rulings turned on the nature of Verizon's services. According to Judge Bates at the District Court level, delivering the opinion in *Verizon I* and *Verizon II*, "[t]he statutory text of the DMCA provides clear guidance for construing the subpoena authority of subsection (h) to apply to all service providers under the Act"[296]. Under section 512(k) the Act provides two definitions of "service provider": "(A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received; (B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)". Given these definitions, the District Court had no doubt that the subpoena power of section (h) was applicable to all service providers, and therefore also applicable to Verizon. Judge Bates held that the narrow definition of section 512(k)(1)(A) was applicable only for subsection (a). In all the other cases, such as section (h), a service provider has to be thought as defined by section

[292] 17 U.S.C. § 512(c): Information residing on systems or networks at direction of users.
[293] The same questions were used by Verizon also in appealing the District Court's orders, see *infra* for explanation. For a discussion on the constitutional problem raised by § 512(h) of the DMCA: M. AMEDEO, *Shifting the Burden: the Unconstitutionality of Section 512(h) of the Digital Millennium Copyright Act and its Impact on Internet Service Providers*, 11 CommLaw Conspectus 311, 317 ff.(2003).
[294] See *Verizon I* and *In re Verizon Internet Services*, 257 F. Supp. 2d 244 (D.D.C. 2003) [*Verizon II*].
[295] *Verizon Appeal*, 1239.
[296] *Verizon I*, 30.

512(k)(1)(A), including the activity of mere transmission of data (such as Verizon's)[297].

On the contrary, Verizon had argued that an essential condition for a valid subpoena under DMCA is a notification to the ISP that complies with subsection (c)(3)(A)[298]. Verizon reasoned that, since subsection (c) deals with "Information Residing on Systems or Networks at Direction of Users", it could not be applied in this case, given that Verizon was simply providing Internet connectivity or acting as a passive conduit[299]. However, in the District Court's view, Verizon's interpretation "would fail significantly to address many of the contexts in which a copyright owner needs to utilize the subpoena process in order to discern the identity of an apparent copyright infringer"[300]. Apparently, liability protection has been given to ISPs in exchange for the assistance in identifying infringers[301]. If the DMCA subpoena were not applicable to mere conduit ISPs then these would receive the liability protection without corresponding obligation to assist copyright owners in the enforcement of their rights[302]. Judge Bates' conclusion, based on the text and structure of DMCA and on the history of the Act, was to grant RIAA's motion to enforce the subpoena and order Verizon to comply with it[303].

But what could have been the solution for the RIAA in case that Verizon's interpretation was correct? Which path could the RIAA follow to enforce the rights of its associates? Verizon's own proposal was to use the so-called "John Doe" actions. Ironically, this became RIAA's next step, as soon as courts started to deny subpoena enforcement[304].

Despite the Court not going through them, Verizon also identified the grounds for possible constitutional challenges to the subpoena power introduced by

---

297 *Verizon I*, 32.
298 17 U.S.C. § 512(h)(2)(A).
299 *Verizon I*, 32.
300 *Verizon I*, 34.
301 "Congress hoped to provide 'greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities'", see *Ellison v. Robertson*, 357 F.3d 1072; 1076 (9th Cir. 2004), citing S. Rep. 105-190, 20 (1998); H.R. Rep. 105-551, pt. 2, 49 (1998). Analyzing DMCA § 152's legislative development, some scholars underline the lobbying activity of both ISPs and copyright holders, such as the RIAA: C. IMFELD, V. SMITH EKSTRAND, *The Music Industry and the Legislative Development of the Digital Millennium Copyright Act's Online Service Provider Provision*, 10 Comm. L. & Pol'y 291 (2005).
302 *Verizon I*, 38.
303 *Verizon I*, 44.
304 See *infra*.

DMCA, a topic better developed in the next suit[305]. Verizon claimed that section 512(h) violates Article III of the Constitution, since it authorizes federal courts to issue a binding process even if there is no pending case or controversy[306].

Article III of the US Constitution refers to the judicial branch[307]. In particular, according to this article the "federal judicial power" is divided into a Supreme Court and other inferior courts that "Congress may from time to time ordain and establish". These courts must function within the specified jurisdictional boundaries of the same article. Section 2 of the article indicates federal courts' subject matter, speaking of "cases" and "controversies". This affirmative grant of power has been read as encompassing also a negative limitation: judicial power cannot extend to anything but a case or controversy[308]. According to the Supreme Court, these words require that litigation is presented to federal courts in an adversarial form and in a context capable of judicial resolution[309]: the matter has to be concrete and not just hypothetical[310]. Verizon's opinion was that this necessary context was lacking.

In Judge Bates' view, the clerk's issuance of a section 512(h) subpoena did not involve the exercise neither of judicial power nor of investigatory power. In case the proposed subpoena is in proper form and has the requirements listed in the section, the clerk shall expeditiously issue and sign the subpoena. This would mean that the clerk only executes a ministerial duty, that is an operation where no discretion is left[311]. To support this interpretation, the Court underlined that for obtaining a section 512(h) subpoena there are rigorous requirements, like the showing of the existence of a breach or violation[312]. Furthermore, "there is simply no basis to conclude that § 512(h) undermines the independence or institutional integrity of the Judicial Branch. Under § 512(h), the district court does not take sides in the copyright holder's request for the alleged infringer's name, but rather, through the

[305] In the same decision were Verizon's stay motion of the Court's order in *Verizon I* and also the motion to quash a second subpoena served by RIAA, since they were both assigned to the same judge, see *Verizon II*, 248.
[306] *Verizon II*, 247. In Verizon's view, § 512(h) also violates the First Amendment right of Internet users, see *infra*.
[307] See J.A. BARRON, C. T. DIENES, *Constitutional Law in a Nutshell*, St Paul, 2005, 18 ff.
[308] K.M. SULLIVAN, G. GUNTHER, *Constitutional Law*, New York, 2007, 31.
[309] *Flast v. Cohen*, 392 U.S. 83, 97 (1968); see also L.H. TRIBE, *American Constitutional Law*, New York, 1988, 67 ff.
[310] SULLIVAN, GUNTHER, *Constitutional Law*, cit., 31.
[311] *Verizon II*, 249.
[312] *Verizon II*, 252.

clerk, serves as a passive, neutral instrument facilitating the attempt to retrieve the name"[313]. According to this interpretation there seems to be no threat to the judicial power.

For all the reported reasons, the District Court denied the motion to quash and the request for a stay presented by Verizon. But Verizon appealed both of the District Court's orders on three different arguments: 1) section 512(h) does not apply to ISP acting as merely conduit; 2) Article III unconstitutionality issue related to the fact that section 512(h) subpoena should not be granted in the absence of a pending case or controversy; and 3) section 512(h) violates the First Amendment because it lacks to protect users' anonymity[314].

The Court of Appeal started its reasoning with the analysis of DMCA safe harbors. The Justices underlined that the notice and take-down provision was significantly absent from section 512(a), regarding ISPs only transmitting, routing or providing connections. As already explained, in order to obtain a subpoena, the claimant must submit "a copy of a notification described in subsection (c)(3)(A)"[315]. The subpoena required by the RIAA could not meet this condition, since Verizon was not storing the infringing material that, in turn, could not be removed or the access to which could not be disabled by the ISP[316]. The infringing material is stored on users' computers that the ISP obviously cannot reach. The RIAA argued that instead of removing the material or disabling the access, Verizon could simply have terminated a user's Internet account. Verizon argued – and the Court of Appeal agreed – that disabling an individual's access to infringing material is different from disabling access to the Internet[317].

The RIAA pointed out that under section 512(c)(3)(A) a notification is effective if it "includes substantially" the required information. With the information given by RIAA, Verizon was able to identify the infringer. According to the RIAA, then, the notice was sufficient. However, the Senate and House Reports read the term

313 *Verizon II*, 255.
314 *Verizon Appeal*, 1231.
315 17 U.S.C. § 512(h)(2)(A).
316 *Verizon Appeal*, 1234.
317 Indeed, as cited in *Verizon Appeal*, 1235, "[w]here different terms are used in a single piece of legislation, the court must presume that Congress intended the terms have different meanings", see *Transbrasil S.A. Linhas Aereas v. Dep't of Transp.*, 253 U.S. App. D.C. 31, 791 F.2d 202, 205 (D.C. Cir. 1986).

"substantially" for the cases in which there were technical or spelling errors[318]. It was clear that the notification made by RIAA was not merely wrong; rather, it could not identify any infringing material at all. Even if the Recording Industry argued that given the definition of ISP under section 512(k)(1)(B), section 512(h) could be applied to all kinds of ISPs. The Court, instead, held that since a notification under section 512(c)(3)(A) was needed and since this notification cannot be done for an ISP such as Verizon, the subpoena could not be issued in the case[319].

Looking at the history of DMCA, both the District Court and the Court of Appeal admitted that, while enacting the Act, Congress did not consider P2P networks, since they came into existence only later[320]. Both of them recognized that it is the unique power of Congress to change copyright law[321]. But, in facing the tricky formulation of section 512, where it was difficult to understand whether it was applicable to Verizon or not, the two courts reached two different outcomes. The District Court thought that it was applicable, and that "[o]therwise, the statute would fail significantly to address many contexts in which a copyright owner needs to utilize the subpoena process in order to discern the identity of an apparent copyright

[318] Senate Rep. N. 105-190, at 47 (1998); House Rep. N. 105-551 pt. II, at 56 (1998). But for a different interpretation see *ALS Scan, Inc., v. RemarQ Cmtys, Inc*., 239 F.3d 619, 625 (4th Cir. 2001): "subsection [§ 512(c)(3)(A)(iii)] specifying the requirements of a notification does not seek to burden copyright holders with the responsibility of identifying every infringing work - or even most of them - when multiple copyrights are involved. Instead, the requirements are written so as to reduce the burden of holders of multiple copyrights who face extensive infringement of their works. Thus, when a letter provides notice equivalent to a list of representative works that can be easily identified by the service provider, the notice substantially complies with the notification requirements".

[319] *Verizon Appeal*, 1236.

[320] "[P]eer-to-peer (P2P) software and "bots," a software tool used by copyright owners to monitor the Internet and detect unauthorized distribution of copyrighted material - were "not even a glimmer in anyone's eye when the DMCA was enacted" by Congress in 1998", see *Verizon I*, 38, citing Brief of *Amicus Curiae* Alliance for Public Technology, et al., at 6; see also *Verizon Appeal*, 1238.

[321] See for example *Verizon I*, 38: "the courts cannot read new provisions or exceptions into a statute in order to accommodate future technological developments. Particularly in the field of copyright, federal courts must defer to Congress' expertise and constitutional authority". *Verizon Appeal*, 1238: "[i]t is not the province of the courts […] to rewrite the DMCA in order to make it fit a new and unforeseen internet architecture. […] The plight of copyright holders must be addressed in the first instance by the Congress; only the "Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology." See *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 431, 78 L. Ed. 2d 574, 104 S. Ct. 774 (1984)". RAYNOLDS, *One Verizon, Two Verizon, Three Verizon, More? – A Comment: RIAA v. Verizon and How The DMCA Subpoena Power Became Powerless*, cit., 376 suggests a different approach, taken by the Supreme Court when facing the appearance of photography. The Copyright Act had not contemplated the possibility of such instrument, but the Court interpreted it in an extensive way. As a consequence Congress amended the Act, which now protects "original works of authorship fixed in any tangible medium of expression, *now known or later developed*" [17 U.S.C. § 102(a); emphasis added].

infringer"[322]. The Court of Appeal, instead, wrote: "[w]e are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights […]. It is not the province of the courts, however, to rewrite the DMCA […] no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries"[323]. On May, 24, 2004, the RIAA filed a Petition for a Writ of Certiorari with the Supreme Court, which was denied[324].

c) After the Verizon cases

The debacle of the RIAA against Verizon was not its only one. Perhaps as a result of the Verizon saga, other ISPs did not comply with the DMCA subpoena served by the RIAA. In particular, two cases were decided on the basis of *Verizon*: one with Charter Communications[325]; the other one with University of North Carolina[326].

As was the case with Verizon, the RIAA obtained a subpoena from the clerk of the District Court of the Easter District of Missouri in order to acquire information regarding around 200 of Charter's subscribers. Charter filed a motion to quash the subpoena, a motion that the District Court denied. Charter then filed a notice of appeal and a motion to stay proceedings. Since the District Court declined to act on the motion to stay within the deadline, Charter filed an emergency motion to stay with the Court of Appeals for the Eight Circuit, which was also denied. As a result, Charter had to comply with the subpoena and gave names and addresses of its customers to the RIAA.

---

322 *Verizon I*, 34.

323 *Verizon Appeal*, 1238.

324 *Recording Ind. Assoc. v. Verizon Internet Servs*., 2004 U.S. LEXIS 6700 (U.S., Oct. 12, 2004); *Verizon Internet Servs. v. Recording Indus. Assoc.of Am., Inc.*, 2004 U.S. LEXIS 6701 (U.S., Oct. 12, 2004).

325 "Charter Communications, Inc. is a Fortune 500 company and the fourth-largest cable operator in the United States. Charter provides advanced video, high-speed Internet, and telephone services to approximately 5.5 million residential and business customers in 27 states", see http://www.charter.com/footer/footerPage.jsp?tag=about.

326 *In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 773 (8th Cir., 2005) [*In re Charter*]. For a general overview of the case see M.R. BOEVE, *Will Internet Service Providers Be Forced to Turn In Their Copyright Infringing Customers? The Power of the Digital Millennium Copyright Act's Subpoena Provision After* In Re Charter Communication, 29 Hamline L.R. 177 (2006) available at http://law.hamline.edu/files/vol29no1article6.pdf. *In re Subpoena to University of North Carolina at Chapel Hill*, 367 F. Supp. 2d 945 (M.D.N.C., 2005) [*In re University N.C.*].

Charter appealed again in front of the same Court of Appeals[327]. Its appeal was built on four arguments:

1) section 512(h) was applicable only to ISPs engaged in storing material and not to Charter, which was engaged simply in transmitting (which is the same argument made by Verizon and approved in *Verizon Appeal*);

2) a subpoena must be supported by a case or controversy, but there was no case or controversy pending when the subpoena was issued (also Verizon's reasoning);

3) the enforcement of section 512(h) could violate the subscribers' privacy, as regulated in the Communication Act of 1934[328];

4) section 512(h) violated the First Amendment right of Internet users (argument that appeared also in Verizon's cases)[329].

In its finding, the majority of the Court of Appeal simply retraced the reasoning of the appellate decision taken in *Verizon* and concluded by agreeing with it[330]. As a consequence, the Court of Appeal did not address the constitutional arguments presented by the ISP. Nevertheless, the Court wrote that section 512(h) "*may* unconstitutionally invade the power of the judiciary"[331].

In this case there was a quite extensive dissenting opinion delivered by Justice Murphy. Justice Murphy criticized the interpretation proposed by Charter and adopted by the Court for it would "block copyright holders from obtaining effective protection against infringement through conduit service providers"[332]. In her view, legal actions against end users are the only practical method for protecting the interests of copyright holders. In her reasons, she underlined that, on the contrary to what was sustained by the reasons in Verizon, peer-to-peer file sharing programs "were already being developed at the time of the congressional hearing preceding the passage of the DMCA"[333]. Justice Murphy held that section 512(h) subpoena may be issued to "a service provider". Since there is no express reference to one or more kinds of service provider, the provision can be applied to all types of ISP. If

[327] *In re Charter*, 774.
[328] 47 U.S.C. § 551(c)(1).
[329] *In re Charter*, 775.
[330] *In re Charter*, 777.
[331] *In re Charter*, 777-778, italics in original.
[332] *In re Charter*, 778.
[333] *In re Charter*, 779.

Congress had intended to restrict the application of section 512(h) only to some types of ISP, then it would have simply stated it clearly[334].

Justice Murphy gave another interpretation of the six elements needed for a the notification under subsection (c)(3)(A)[335]. Particularly, she focused on the third element: "(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material". According to Justice Murphy's opinion, "[t]he subsection defines the material to be identified in two ways: (1) material that is 'claimed to be infringing' and (2) material that is 'the subject of infringing activity and that is to be removed or access to which is to be disabled'"[336]. The distinction – set by the conjunction "or" – would be carrying forward the differentiation between section 512(a) about conduit ISPs and sections 512(b) – (d) about storage ISPs. A conduit ISP could indirectly disable access to material by simply terminating the account of an infringer[337]. Justice Murphy claimed that the majority's interpretation would shield ISPs from liability without the exchange of their assistance in the enforcement of copyright[338].

Justice Murphy also addressed in passing the third of Charter's above listed arguments, the one on users' privacy. The DMCA states that the ISP must immediately disclose the information required by the subpoena, "notwithstanding

---

334 *In re Charter*, 780.

335 17 U.S.C. § 512(c)(3)(A): "To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following: (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site. (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material. (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted. (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law. (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed".

336 *In re Charter*, 780-781.

337 *In re Charter*, 781.

338 *In re Charter*, 782.

any other provision of law"[339]. In her interpretation, this means that the subpoena is intended to "supersede […] other statutes that might interfere with or hinder the attainment of [its] objective"[340]. This would mean that ISP can comply with the subpoena without violating the Cable Act.

The RIAA also failed to obtain a subpoena in *In re University N.C.* In the matter, the Recording Industry ascertained that some individual screen names were illegally downloading songs with P2P software. These individuals were connecting to the internet through the University of North Carolina at Chapel Hill or through North Carolina State University. The universities were acting as ISPs, namely as "merely transmitting" ISPs. The RIAA obtained a subpoena from the clerk[341] directed to the universities. Initially the two institutions appeared willing to comply and notified the users that the subpoena had been issued. The two users, whose nicknames were "hulk" and "CadillacMen", filed a motion to intervene as John and Jane Doe as well as a motion to quash the subpoena[342]. Both of these defendants raised statutory and constitutional arguments to quash the subpoena[343]. In particular the Does used the same argument employed by Verizon: since an ISP only transmitting information cannot be subject to a notification like the one in section 512(c)(3), and given that the DMCA requires this notification for the issue of a subpoena, section 512(h) cannot be applied in their cases.

The RIAA asked the judges to look beyond the words of the Act and to embrace the congressional intent, which was to curtail internet violations. Therefore section 512(h) should be applied also to section 512(a) providers. The Recording Industry said, once again, that subsection (h)(2)(A) was satisfied as well by "supplying the substantial equivalent of the information contained in a notification"[344].

The District Court's decision was based on *Verizon* and *In re Charter*. The Court reasoned that in the mentioned cases courts were actually reading section

[339] 17 U.S.C. § 512(h)(5).
[340] Judge Murphy cited *Campbell v. Minneapolis Pub. Hous. Auth. ex rel City of Minneapolis*, 168 F.3d 1069, 1075 (8th Cir. 1999), see *In re Charter*, 785.
[341] Clerk of the District Court for the Middle District of North Carolina.
[342] *In re University N.C.*, 946.
[343] Defendant "Jane Doe" also raised procedural arguments, which will be not touched here, see *In re University N.C.*, 956 ff.
[344] *In re University N.C.*, 952.

512(h)(2)(A) in an expansive manner. Indeed, since letter (h) mentions only letter (c), "a narrow reading would have found that only Section 512(c) providers were covered"[345]. This wider reading of section 512(h) is possible because with regard to sections 512 (b) and 512(d) ISPs there are applicable notification provisions. On the contrary applying section 512(h) to section 512(a) ISPs – such us universities – would require the Court to craft rules[346]. As previously stated, the Does argued that the fact that it is a clerk who issues the subpoena is a violation of judicial power. The RIAA, following the *Verizon I* decision, argued that clerk's intervention was merely a ministerial duty. The Court disagreed: the fact that section 512 (h) is ambiguous would lead the clerk in an interpretation that would result in his function being more-than-ministerial[347]. Following this reasoning the Court ordered both subpoenas to be quashed[348].

d) The "John Doe" phase

As has been noted, Verizon argued that, even if the subpoena was not applicable in its cases, copyright holders could still make use of "John Doe" actions[349]. The idea of Verizon's was that these actions would better protect users' rights and service providers could have the opportunity to seek to quash the subpoena. The trial decision in *Verizon I* explained that such an action would require

---

345 *In re University N.C.*, 953.

346 *In re University N.C.*, 954. See also *Ibidem* at 955: "[c]ongress explicitly tied the subpoena power to receipt of a notification which arguably applies to Sections 512(b)&(d) service providers, but clearly does not apply to Section 512(a) service providers".

347 *In re University N.C.*, 955.

348 The decisions of *Verizon Appeal*, *In re Charter* and *University N.C.* have been widely criticized, see for example: Z. CHAFFEE-MCCLURE, *Train in Vain: The Clash Between the RIAA and the Eight Circuit over Whether the DMCA Subpoena Provision Applies to Peer-to-Peer Networks, and the Need to Steer the DMCA Back on Track with Congressional Intent* [*In re Charter Commc'ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771 (8th Cir. 2005)], 45 Washburn L.J 175, 189 (2005); RAYNOLDS, *One Verizon, Two Verizon, Three Verizon, More? – A Comment: RIAA v. Verizon and How The DMCA Subpoena Power Became Powerless*, cit., 376; BOEVE, *Will Internet Service Providers Be Forced to Turn In Their Copyright Infringing Customers? The Power of the Digital Millennium Copyright Act's Subpoena Provision After* In Re Charter Communication, cit., 137 ff; DUTCHER, *A Discussion of the Mechanics of the DMCA Safe Harbor and Subpoena Power, as Applied in* RIAA v. Verizon Internet Services, cit., 502 ff, spec. 514, where the authors argues that the approach taken by these courts would violate "equal protection", since users of a § 512(a) ISP would be treated differently from users of § 512(b)-(d) ISPs.

349 The actual, typical scenario of music download lawsuit is commenced by the record companies before federal courts, against Does with common ISP, in the jurisdiction where the ISP is located. In this way the suit normally joins tens or even hundreds of defendants, grouped by ISP. For the implications of such approach see J.M. DICKMAN, *Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits*, 82 Tulane L. R. 1049 (2008).

a great deal of effort and expense for the copyright holders, while the section 512(h) subpoena was easier and less costly[350]. The former would also be slower, and "undermine the ability of copyright owners to act quickly to prevent further infringement"[351]. On the other hand, the appellate decision in *Verizon* stated that DMCA subpoena would be more protective for users, given the requirements that had to be fulfilled by the copyright holder prior to successfully obtaining an injunction[352].

Merely one month later, the RIAA changed strategy, deciding to "accept the proposal" to use the "John Doe" proceeding. This change in the RIAA's strategy probably came directly from the less-than-satisfactory results obtained through the DMCA subpoena proceedings in *Verizon*, given the authority and influence of the decision rendered by the U.S. Court of Appeals for the District of Columbia Circuit, and in a situation where *certiorari* to the Supreme Court was denied. Indeed, as we have seen, its reasons were in fact immediately followed by another court of appeal in the *In re Charter* case[353].

The "John Doe" action consists of an "*ex parte* discovery"[354]. *Ex parte* processes are those where one of the parties has not been notified of the existence of the process, and therefore is neither present nor represented. Through this process, a party (the RIAA in this case) can obtain an "immediate discovery" which authorizes it to serve the counterparty (Verizon) with a subpoena for the production of the true identities behind the IP dynamic addresses[355].

---

[350] See also RAYNOLDS, *One Verizon, Two Verizon, Three Verizon, More? – A Comment: RIAA v. Verizon and How The DMCA Subpoena Power Became Powerless*, cit., 371 ff.

[351] *Verizon I*, 40.

[352] *Verizon I*, 41. In the case *In re Charter*, the Court realized that, due to its interpretation of DMCA "copyright owners [could not] deter unlawful peer-to-peer file transfers unless they [could] learn the identities of persons engaged in that activity". To solve this problem, the same Court suggested that "organizations such as the RIAA [could] also employ alternative avenues to seek this information, such as "John Doe" lawsuits", see *In re Charter*, 775. See also M. FROOMKIN, *Anonymity and the Law in the United States*, in I. KERR, V. STEEVES, C. LUCOCK (eds.), *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York, 2009, 441, spec. 453.

[353] The RIAA had to change its strategy or, alternatively, it had to demonstrate that the subpoenaed ISP could be classified under § 512(b)-(d).

[354] *Entry: Ex parte*, BLACK, *Black's Law Dictionary*, cit., 517: "A judicial proceeding, order, injunction, etc., is said to be *ex parte* when it is taken or granted at the instance and for the benefit of one party only, and without notice to, or contestation by, any person adversely interested". For what discovery concerns, it is a "pre-trial devices that can be used by one party to obtain facts and information about the case from the other party in order to assist the party's preparation for trial", cf. *Entry: Discovery*, BLACK, *Black's Law Dictionary*, cit., 419.

[355] BACKERMAN, *How the RIAA litigation process works*, cit.

The RIAA has thus tried different ways to pursue the goal of punishing illegal P2P networks and users, the most important of which as we have seen are the lawsuits against ISPs and colleges. Some colleges were cooperative with the Recording Industry Association, forwarding the letters to their students[356]. Others were not, as noted in the UNC and NC State cases above discussed[357]. Indeed, starting from 2007, the RIAA has sent hundreds of "pre-litigation" letters to various universities, with the request to forward them to their students. These letters did not identify the infringers; they just contained their IP addresses. With the threat of a future suit with damages upwards of $750, they offered a settlement of about $3,000, as long as the student paid within twenty days after receiving the letter[358]. Only if the student did not respond to this settlement offer letter, the RIAA started with the "John Doe" phase. Once the RIAA got users' names and addresses, it stopped with the John Doe lawsuits and either sent letters to users for a settlement or started suing the identified defendants.

In the latter case, the RIAA usually exploited a template complaint accusing the defendant of "downloading, distributing, and/or making available for distribution" a list of songs. When a defendant defaulted, plaintiffs usually obtained a default judgment[359], with a value per each song roughly 1000 times the amount the defendant could have purchased the song[360]. There have been several claims filed, but it seems that only two eventually went to trial[361].

---

[356] Some university even fined their students upon the receipt of these letters, see EFF, *RIAA v. The People: Four Years Later*, cit., 9.

[357] See also already cited *In re University N.C.*

[358] EFF, *RIAA v. The People: Four Years Later*, cit., 8-9. This campaign was at some time been supported through a website (http://www.p2plawsuits.com) where individuals receiving pre-litigation letters could simply settle their cases with a credit card payment; *Ibidem*, 9.

[359] Default judgments may exist in three different types of situations. In the first one, the defendant never appears or answers to plaintiff's complaint (like in the cases here told); in the second, despite making an appearance, the defendant fails to file a formal answer; in the last one the defendant fails to comply with one or more procedural requirements, see J.H. FRIEDENTHAL, M.K. KANE, A.R. MILLER, *Civil Procedure*, St Paul, 2005, 480 ff; see also *Entry: Default-judgment*, BLACK, *Black's Law Dictionary*, cit., 376, according to which "[u]nder Rules of Civil Procedure, when a party against whom a judgment for affirmative relief is sought has failed to plead (*i.e.* answer) or otherwise defend, he is in default and a judgment by default may be entered by the clerk or the court".

[360] For a critic on the award these damages see J.C. BARKER, *Grossly Excessive Penalties in the Battle against Illegal File-Sharing: The Troubling Effects of Aggregating Minimum Statutory Damages for Copyright Infringement*, 83 Texas Law Review 525, 2004.

[361] *Virgin Records Am., Inc. v. Thomas*, 2007 U.S. Dist. LEXIS 79585 (D. Minn. 2007), then renamed *Capitol Records Inc. v. Thomas*, 579 F. Supp. 2d 1210 (2008) and *Sony BMG Music Entm't v. Tenenbaum*, 672 F. Supp. 2d 217 (D. Mass. 2009). For a concise story of RIAA's suits and their endings see BACKERMAN, *How the RIAA litigation process works*, cit.

In 2003, along with the first lawsuits, the RIAA announced an amnesty program, called the *Clean Slate Agreement*. With this program "files-sharers [could] avoid lawsuits if they sign[ed] a declaration pledging that they [would] delete all copyrighted music files from their hard drives and mp3 players and never again share or download music illegally. The amnesty program [was] only available to people who the RIAA ha[d] not yet sued or subpoenaed"[362]. The program was harshly criticized. According to the EFF, under the *NET Act* the declaration could be used against the signer as an admission of violating copyright. Moreover, this amnesty would have covered only suits by the RIAA, but not by other copyright holders[363].

In December 2008, the RIAA announced that it would stop suing people as a way to fight illegal file-sharing. In the meantime, to reach the same result, the RIAA tried to find agreements with ISPs[364]. This is known as the "graduated response plan" or "three strikes". The RIAA finds IP addresses of infringers and notify them to ISPs. ISPs will contact the user and give her three chances to stop the infringing behavior. If she does not stop, then the ISP will cut off her Internet access directly through the server[365].

---

[362] Quotation from EFF, *Recording Industry Announces Lawsuits Against Music Sharers*, 2003, available at http://w2.eff.org/IP/P2P/20030908_eff_pr.php.

[363] See EFF, *Why the RIAA's "Amnesty" Offer is a Sham*, 2004, *http://w2.eff.org/share/amnesty.php*.

[364] G. ZILKHA, *The RIAA's Troubling Solution to File-Sharing*, 20 Fordham Intell. Prop. Media & Ent. L.J. 667, 688 (2010).

[365] See D.A. MCGILL, *New Year, New Catch-22: Why the RIAA's Proposed Partnership with ISPs Will Not Significantly Decrease The Prevalence of p2p Music File Sharing*, 29 Loy. L.A. Ent. L. Rev. 353 (2009). This new "strategy" has gained a lot of critics, mainly because of the "fundamental-right-approach" increasingly given to the (right to) access to the Internet. Furthermore, this approach could heavily influence the existence of small ISPs, which could not be strong enough to bear the costs of their consumers' access cuts or to survive secondary copyright liability trials. See ZILKHA, *The RIAA's Troubling Solution to File-Sharing*, cit., 689 ff. Since the first moves of RIAA, dozens of commentators have tried to propose different solutions to the issue of illegal file-sharing. For some proposal see: ZILKHA, *The RIAA's Troubling Solution to File-Sharing*, cit., 706 ff; P. FOGARTY, *Major Record Labels and The RIAA: Dinosaurs in a Digital Age?*, 9 Hous. Bus. & Tax L.J. 140, 170 ff. (2008); D. REYNOLDS, *The RIAA Litigation War on File Sharing and Alternatives More Compatible With Public Morality*, 9 Minn. J.L. Sci. & Tech. 977, 987 ff. (2008); SCHULTZ, *The False Origins of the Induce Act*, cit., 559 ff.; J. BOAG, *The Battle of Piracy versus Privacy: How the Recording Industry Association of America (RIAA) is Using the Digital Millennium Copyright Act (DMCA) As Its Weapon Against Internet Users' Privacy Rights*, 41 California Western Law Review 241, 266 ff. (2004); D.J. GERVAIS, *The Price of Social Norms: Towards a Liability Regime for File-Sharing*, 12 J. Intell. Prop. Law 39, 55 ff. (2004); N.W. NETANEL, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 Harv. J.L. & Tech. 1, 31 ff. (2003); D.J. GERVAIS, *Application Of An Extended Collective Licensing Regime In Canada: Principles And Issues Related To Implementation*, Study Prepared for the Department of Canadian Heritage, 2003, available at: http://aix1.uottawa.ca/~dgervais/publications/extended_licensing.pdf. MCGILL, *New Year, New Catch-22: Why the RIAA's Proposed Partnership with ISPs Will Not Significantly Decrease The Prevalence of p2p Music File Sharing*, cit., 360 argues that a solution would be "making file sharing a

e) Recent developments in the battle against file sharing

As previously mentioned, the RIAA has recently started to sue P2P software producers once again. In the wake of the *Grokster* decision, the Recording Industry feels that it can now win these cases more easily. In the meantime, however, the RIAA has not stopped suing also individual users with the "John Doe tactic". The RIAA is not alone in the battle against infringers, since also the Motion Pictures Association of America (MPAA) and film makers have been giving a hard time to file sharers insofar as movies are concerned. Here, I shall here give a brief account of some of these most recent developments.

In 2008 Arista Records and many other recording companies sued some John Does following the same path previously blazed by the RIAA[366]. Plaintiffs alleged that defendants had used a P2P program to download and distribute plaintiffs' copyrighted works to the public without authorization. As usual, Arista could discover the IP addresses of users, but not their names; therefore, they were unable to subpoena the ISPs to obtain that data. In particular, those IP addresses were distributed by the California State University of Fresno, which acted as the ISP. In deciding the motion, Judge Austin acknowledged that the US courts did not have a unique vision on the feasibility of discovery in these processes and cited as many decisions in favor of disclosure as against disclosure[367]. Judge Austin decided that disclosure could be granted, including names, current and permanent addresses, telephone numbers, email addresses, and Media Access Control addresses for each defendant as identified by the IP numbers listed in the Complaint. Nevertheless, Judge Austin, in order to protect the Does' privacy right, wanted the University to inform its subscribers about the subpoena, so that they at least had the opportunity to bring a motion to quash it[368].

---

criminal, rather than a civil matter". I disagree with this Author for many reasons, one of which is that Italian system, where illegal file-sharing is punished as a crime, is the proof that this would not work. Indeed we cannot say there has been a decline in the volume of P2P exchange of files (the same could anyway be said for the US system, where criminal remedies have been existing since the 19th Century). Up to now it seems that the RIAA has a sort of deaf ear for these proposals.

[366] *Arista Records, LLC v. Does 1-12*, 2008 U.S. Dist. LEXIS 82548.

[367] *Arista Records, LLC v. Does 1-12*, cit., 3-4.

[368] *Arista Records, LLC v. Does 1-12*, cit., 6.

That same year, the same companies sued other John Does, subscribers of State University of New York at Albany (SUNY Albany)[369]. Arista alleged that Does shared and distributed files through a P2P technology, without copyright owners' permission. To obtain the IP addresses, the recording companies relied on MediaSentry. On July 2008, the District Court granted Arista permission to seek discovery from SUNY Albany, which notified each Doe with the intention to disclose the requested information. Four defendants responded in order to quash the subpoena, raising a number of defenses, one of which related to the infringement of First Amendment. The Court, as other courts had already done, claimed that even if on the internet users have a right to anonymity under First Amendment, this is a very limited right since P2P is not a real way to express oneself. The privacy right would also be very limited[370]. Furthermore Judge Treece held that, even if the defendants had the aforementioned rights, these should nevertheless be balanced against copyright owners' right to disclosure. Applying the test laid down in *Sony Entertainment* the court reasoned that, since P2P download is copyright infringement[371], plaintiffs' discovery was reasonable. "The Subpoena [sought] the IP user's name, address, telephone number, email address, and MAC, and nothing else that would be considered intrusive"[372]. Since subpoenas were the only way to obtain this data, and that the defendants had a minimal expectation of privacy[373], the Court found that granting the motion was the correct solution and that Does' First Amendment right to anonymity should have given way to plaintiffs' right to use discovery. For these reasons, the Court ordered SUNY Albany to effect the disclosure of users' data.

More recently, the MPAA has also started to move against P2P file-sharing. One of the most well-known cases is the one related to the movies "Far cry" and

[369] *Arista Records, LLC v. Does 1-16,* 2009 U.S. Dist. LEXIS 12159.
[370] *Arista Records, LLC v. Does 1-16,* cit., 12.
[371] To support this claim the court cited the Grokster case.
[372] *Arista Records, LLC v. Does 1-16,* cit., 20.
[373] Conceptually, the notion of allowing others to have access to one's database by virtue of the Internet, in order to pluck from a computer information and data that the computer owner or user wishes to share, renders void any pretext of privacy, cf. *Arista Records, LLC v. Does 1-16,* cit., 21. In particular: "[the defendants] are not in the position of even arguing that they had an expectation of privacy. If the allegation that the Doe Defendants placed copyrighted recording into index files for others to take at will and hereby trampled upon the exclusive owner's copyright domain are true, they have forfeited any expectation of privacy they may have had", *Ibidem*, 24.

"The Hurt Locker"[374]. In the spring of 2010, a Washington law firm, calling itself the "U.S. Copyright Group" (USCG), started a series of lawsuits against BitTorrent users. The lawsuits involved unnamed John Does and subpoenas to ISPs to obtain users' identities, exactly the same way the RIAA had done[375]. The suits implicated more than 14.000 people[376]. In the hearing of *Achte/Neunte v. Does*, Judge Collyer was concerned with the defendants' interest to be protected, so she ordered that the plaintiffs Achte/Neunte and its amici work together to draft a notice to be sent to users whose personal data were being sought[377]. She was indeed worried that the Does could not raise legal objections[378]. The case is ongoing and is far from being concluded.

As said above, suits against individuals are not the only way for copyright owners to fight file sharing. The recording industry, together with motion pictures companies, have recently gone back to the battle against P2P software producers. One example is the case of LimeWire[379]. In the *Lime* Wire case, the plaintiffs are thirteen major record companies raising various claims of secondary copyright infringement against Lime Wire LLC, its chairman and the holding group (Lime Wire FLP), for their role in distributing the LimeWire software program[380]. As for copyright infringement, the record companies have introduced three claims: inducement of copyright infringement; contributory copyright infringement and vicarious copyright infringement. Furthermore, the record companies also claim also

[374] As it will be explained in the next chapter, copyright owners of this movie have been suing people also in Canada.
[375] Cf. https://www.eff.org/cases/uscg-v-people.
[376] Cf. https://www.eff.org/cases/achte-neunte-v-does and https://www.eff.org/deeplinks/2010/06/judge-orders-user-friendly-notices-does-targeted; see also http://filesharingz.com/news/198198/22_000_alleged_39_Hurt_Locker_39_pirates_are_let_off_the_hook.html.
[377] *Achte/Neunte v. Does 1-4.577*, 2010 U.S. Dist. LEXIS 128233.
[378] https://www.eff.org/deeplinks/2010/06/judge-orders-user-friendly-notices-does-targeted.
[379] *Arista Records, LLC v. Lime Group, LLC*, 715 F. Supp. 2d 481 (2010) [*LimeWire*]. See also the cases of eDonkey - *Arista Records LLC v. MetaMachine, Inc*., No. 06-cv-06991, 2006 U.S. Dist. Ct. Pleadings 6991 (S.D.N.Y. September 11, 2006). Parties settled and the website was later shut down. See C. MCCARTHY, *File-sharing site eDonkey kicks it, CNET News.com*, September 13, 2006, at http://news.cnet.com/File-sharing-site-eDonkey-kicks-it/2100-1030_3-6115353.html.
[380] LimeWire is a P2P software which permits the sharing of digital files over the Internet. In particular, LimeWire is based on the "Gnutella network". As it happens in many other P2P software, when a user enters a query into the search function on LimeWire's interface, the software scans the computers connected to the network and locates files that matched the query. The user can then download any of these files. Through LimeWire there is a transfer of a digital copy of the file from a computer to another.

common law copyright infringement for sound recordings published before 1972381. In May 2010, the District Court granted summary judgment to the record companies.

Regarding secondary copyright infringement, the plaintiff record companies had to first demonstrate the existence of a direct copyright violation, i.e. an infringement by LimeWire users. Relying on expert testimony, the Court held there were no doubts that LimeWire users had infringed the plaintiffs' copyrights. Judge Wood found particularly significant the fact that the recording industry had already sued LimeWire users directly382. In the Court's opinion, the plaintiff record companies had proved that they owned copyright in the works allegedly shared and that these were exchanged through the LimeWire network383. Once stated that final users had infringed plaintiffs' copyright, the Court analyzed LimeWire's secondary liability.

Applying the *Grokster* decision, Judge Wood investigated whether the defendants had engaged in an inducement of infringement and, in particular, whether they engaged in purposeful conduct encouraging copyright infringement and with the intent to encourage such infringement. The Court held that the group had created and distributed LimeWire so that users could commit substantial infringements. Moreover, on the basis of many pieces of evidence, the District Court Judge found that the LimeWire defendants were aware of this substantial infringement. The Judge based her findings on the fact that defendants knew of substantial infringement by users. LimeWire also had made efforts to attract users, enabling and assisting them in the infringement. LimeWire group's business success depended on infringing activities and they failed to mitigate these illicit actions[384].

As for contributory infringement, the Court applied *Sony Betamax* rule: therefore even if LimeWire had materially contributed in users' infringement, it would not be held liable if it was capable of substantial non-infringing uses or was

[381] *LimeWire*, 492.
[382] *LimeWire*, 506.
[383] In particular it seems that plaintiffs had used a "hash" to determine whether a particular file was exchange with LimeWire. In the words of the court "[a] hash is a property of a particular digital file that reflects all aspects of that file, including its content, quality and resolution, length, encoding, and any "ripping" software that has been used to transfer the file. Thus, two audio files with the same hash not only have the same sound content but also have been created using the same "ripping" software. Based on a hash-based analysis, it is clear that copyrighted digital recordings downloaded through LimeWire by Plaintiffs' investigators, were previously digitally shared and downloaded by other LimeWire users"; cf. *LimeWire*, 507 note 21.
[384] For the detailed explanation of these factors see *LimeWire*, 509 ff.

widely used for legitimate, unobjectionable purposes[385]. Making reference to *Grokster*, Judge Wood pointed out that the Supreme Court did not take a clear and unique position on the non-infringing uses of Grokster. Even if LimeWire was used predominantly for infringing purposes, LimeWire had presented evidence that non-infringing contents were exchanged among users, such as public domain works or digital music recordings from musicians trying to promote themselves. Hence, Judge Wood could not determine whether LimeWire software was or not capable of substantial non-infringing uses and denied plaintiffs' motion for summary judgement on this point[386].

LimeWire could be found vicariously liable since it had the right and ability to supervise and control its users and gained a direct financial interest from the infringing activity. The Court found that LimeWire had the ability to limit the use of its products for infringing purposes. In fact, it emerged from evidence that LimeWire had developed filtering systems and could deny access, as well as supervise and regulate users; but they never did any of these supervisory activities. Furthermore, the LimeWire group profited from its ability to attract infringing users, which meant higher advertising revenues. Nevertheless, since Judge Wood could not decide on the existence of substantial non-infringing uses of LimeWire, she did grant not summary judgment on this point either[387].

Lastly, the District Judge decided on the infringement of sound recordings made prior to 1972, protected only by state common law[388]. Basing the decision on New York common law, which requires 1) the existence of a valid copyright and 2) unauthorized reproduction of the protected work, Judge Wood found defendants liable for this claim[389].

Thus, in the end, LimeWire group was held to be liable for inducing infringement and for infringing common law copyright. For these claims the District Court granted the motion[390]. In October of that same year, Judge Wood issued a permanent injunction against LimeWire. The injunction, which is broad and wide,

[385] *LimeWire*, 516, citing *Sony Betamax Supreme Court*, 442.
[386] *LimeWire*, 517-518.
[387] *LimeWire*, 518-519.
[388] Cf. 17 U.S.C. § 301(c).
[389] *LimeWire*, 519-520.
[390] There were also other claims, such as unfair competition, see *LimeWire*, 520 ff.

imposes on the defendant the obligation to totally refrain from any infringing activity on copyrighted works[391]. Later on, in March 2011, LimeWire reached a settlement with one of the plaintiffs[392]. Despite having shut down the service result of the permanent injunction, the LimeWire group is still defending itself from other plaintiffs' claims.

As shown, the legal battle to stop file-sharing is far from reaching a conclusion as it is the determination of file-sharers to fight back with new technologies[393].

2.3.4 Anonymity, Privacy Concerns and the Need for Balance

So far we have been telling the history of the RIAA's law suits against ISPs, P2P software companies and, to some extent, end-users. The previous sections are meant to furnish the background on which we can now describe some privacy concerns that have arisen in those processes, especially in respect of the application of the DMCA subpoena. Some authors have pointed out that section 512(h) subpoena could be misused. On the one hand, given the easy way in which a person can obtain a subpoena from a clerk[394], malicious people might use it for nefarious purposes[395].

---

[391] *Arista Records, LLC v. Lime Group, LLC*, 2010 U.S. Dist. LEXIS 115675. See in particular pages 21 ff., where Judge Wood clearly states what the defendants should concretely do.

[392] See http://www.reuters.com/article/2011/03/08/us-limewire-settlement-idUSTRE7274O520110308 and http://www.techspot.com/news/42728-limewire-reaches-settlement-with-music-publishers.html.

[393] For an analysis of the possible future of the battle against P2P considering also clouding computing, see A. BRIDY, *Why Pirates (Still) Won't Behave: Regulating P2P In The Decade After Napster*, 40 Rutgers Law J. 565 (2009), 588 ff

[394] See the already mentioned requirements under 17 U.S.C. § 512(h).

[395] BOAG, *The Battle of Piracy versus Privacy*, cit., 243. The same worry was underlined by Senator Brownback when discussing the bill "Consumers, Schools, and Libraries Digital Rights Management Act" in 2003. Referring to the District Court's decision on Verizon, the Senator said: "This legislation responds directly to ongoing litigation between the Recording Industry Association of America and Internet service providers Verizon and SBC Communications. This litigation has opened wide all identifying information an ISP maintains on its subscribers, effectively requiring ISPs to make that information available to any party simply requesting the information. The legislation also creates certain minimal protections for consumers legally interacting with digital media products protected by new digital rights management technologies. [...] It has been determined by a Federal court that a provision of the Digital Millennium Copyright Act permits the RIAA to obtain this ISP subscriber's identifying information without any judicial supervision, or any due process for the subscriber. Today, right now, solely due to this court decision, all that is required for a person to obtain the name and address of an individual who can only be identified by their Intent Protocol address—their Internet phone number—is to claim to be a copyright owner, file a one page subpoena request with a clerk of the court, a declaration swearing that you truly believe an ISP's subscriber is pirating your copyright, the clerk will then send the request to the ISP, and the ISP has no choice but to divulge the identifying information of the subscriber—name, address, phone number—to the complaining party. There are no checks, no balances, and the alleged pirate has no opportunity to defend themselves. My colleagues,

On the other hand, it has also been the case that copyright holders have made enormous mistakes in attempting to use the subpoena[396].

Scholars were not the only ones worried by the application of the DMCA subpoena. In 2003 Pacific Bell Internet Services (PBIS) filed suit against the RIAA and two media companies[397], because the ISP had received nearly 200 subpoenas. PBIS was worried that anyone could request private information of users using the subpoena. In the ISP's view this was a threat to the privacy of its customers. One of the defendants was a gay-themed adult entertainment company. Obviously an even greater threat is linked to gay-themed adult porn: once somebody's name has been linked to gay pornography, it would be impossible for her to regain her privacy, even if the allegation were completely false[398]. In another case[399], a "Doe" trying to quash a subpoena argued that the response to the subpoena would reveal protected information regarding users. The Court stated that plaintiff may request "only [*sic!*] the name, address, telephone number, email address and media access control address for each unknown Defendant"[400]. In *Verizon II*, the defendant also argued that DMCA subpoena authority was overbroad and could have a chilling effect on anonymous speech[401].

As already mentioned, First Amendment to the United States Constitution provides: "Congress shall make no law abridging […] the freedom of speech". Since this provision is "simple and unqualified", its interpretation has been broad and wide. What has always been clear is that not every expression or communication can be

this issue is about privacy not piracy. The real harm here is that nothing in this quasi-subpoena process prevents someone other than a digital media owner—say a stalker, a pedophile, a telemarketer or even a spammer from using this quasi-subpoena process to gain the identity of Internet subscribers, including our children. In fact, we cannot even limit this subpoena process to mainstream copyright owners", see Congressional Record - Senate, September 16, 2003, S11571 ff.

396 See BOAG, *The Battle of Piracy versus Privacy*, cit., 258 ff; KAO, *RIAA v. Verizon: Applying the Subpoena Provision of the DMCA*, cit., 423.

397 *Pacific Bell Internet Servs. v. RIAA, Inc.*, 2003 U.S. Dist. LEXIS 21659 (N.D. Cal. 2003). The defendant companies were Mediacentry, Inc. and Titan Media, Inc. The former offers anti-piracy services to entities with copyrighted works (see *Pacific Bell Internet Servs. v. RIAA, Inc.*, cit., 10), while Titan is a San Francisco-based multimedia company engaged in the production of erotic films (see *Pacific Bell Internet Servs. v. RIAA, Inc.*, cit., 6).

398 See BOAG, *The Battle of Piracy versus Privacy*, cit., 254.

399 *Laface Records, LLC et al v. Does 1-5*, 2008 U.S. Dist. LEXIS 13638 (W.D. Mich. 2008).

400 *Laface Records, LLC et al v. Does 1-5*, cit., 10.

401 This defense was also one of Napster's (*Napster I*, 922).

included within the freedom of speech[402]. The Supreme Court has interpreted this right is a core right with the power to entail other ancillary rights. In particular, the Court first recognized the right to speak anonymously in *Talley v. California*[403]. A Los Angeles city ordinance had made it illegal to distribute leaflets, unless they identify the people who created and handed them out. The Court held that the identification requirements would have restricted freedom of expression: people with an unpopular opinion might have been deterred from speaking[404]. In *McIntyre v. Ohio Elections Commission*, the Supreme Court wrote: "[t]he right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse"[405].

As noted above, Verizon argued that DMCA subpoena violated users' First Amendment rights by uncovering their anonymity. Indeed, courts have recognized that the First Amendment covers also expression on the internet[406]. Judge Bates admitted that courts had also "acknowledged some limitations on the subpoena power when its invocation affects First Amendment rights involving anonymity"[407]. Nevertheless, it seemed to the Judge that in those cases the core was First Amendment expression[408]. Furthermore the DMCA subpoena would have reached only the identity of the users and would have not touched the underlying expression[409]. In Judge Bates' view, the procedural requirements under section 512(h), were a sufficiently high burden so as to act as a warranty against the unfounded disclosure of users' identities[410].

---

402 SULLIVAN, GUNTHER, *Constitutional Law*, cit., 741; BARRON, DIENES, *Constitutional Law in a Nutshell*, cit., 373.
403 *Talley v. California*, 362 U.S. 60 (1960)
404 *Talley v. California*, cit., 64-65.
405 *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995).
406 *Reno v. ACLU,* 521 U.S. 844, 870 (1997).
407 *Verizon II*, 259; see *infra*.
408 *Verizon II*, 259-260.
409 *Verizon II*, 262.
410 *Verizon II*, 263-264. The District Court further argues that those of § 512(h) are precisely the kind of requirements that courts have imposed in non-copyright cases to compel an ISP to reveal the identity of anonymous users, see *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999) [*Seescandy.com*]; *In re Subpoena Duces Tecum to America Online, Inc*., 52 Va. Cir. 26 (Va. Cir. Ct. 2000).

As for the overbreadth doctrine some further explanation is needed. This doctrine differs from the usual constitutional challenge, which points to the validity of the law as applied to the particular plaintiff. In the latter case, if there is a judicial determination of unconstitutionality, it does not render the law itself completely invalid; rather, it only makes inoperative that particular application. But the litigant can also challenge the validity of the law itself, by arguing that the law is unconstitutional on its face, because it is overbroad[411]. The overbreadth doctrine has regard to the precision of law, and the tailoring of its effects to the desired legislative goals. A law limiting free speech may be clear on its face, but might indiscriminately reach both protected and unprotected expressions. In this sense it may "sweep too broadly". With such a kind of over-reaching law, protected expression could be chilled or suppressed[412]. Therefore, in these cases, the challenged statute is wiped out with respect to all possible applications[413].

The District Court held that even if one could imagine some speculative application of the subpoena that might be overbroad, this was not sufficient. Furthermore, according to Judge Bates, the phenomenon of file-sharing had caused the recording industry to suffer substantial losses. "Whatever marginal impact the DMCA subpoena authority may have on the expressive or anonymity rights of Internet users, then, is vastly outweighed by the extent of copyright infringement over the Internet through peer-to-peer file sharing, which is the context of the legitimate sweep of § 512(h)"[414]. The Court further underlined that when an individual opens his or her computer to permit others, through P2P systems, to download music from that computer, "it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world"[415].

Not all courts have reasoned in this way. In *Capitol Records, Inc. v. Does 1-16*[416] Judge Garcia underlined that the "disclosure of subscriber log files may contain highly confidential and sensitive files, disclosure of which could well be violative of the subscribers' privacy rights". This file could include credit card information,

411 BARRON, DIENES, *Constitutional Law in a Nutshell*, cit., 382; TRIBE, *American Constitutional Law*, cit., 1022 ff.
412 BARRON, DIENES, *Constitutional Law in a Nutshell*, cit., 383.
413 C. MASSEY, *American Constitutional Law: Powers and Liberties*, New York, 2001, 1043.
414 *Verizon II*, 265-266.
415 *Verizon II*, 267.
416 *Capitol Records, Inc. v. Does 1-16*, 2007 U.S. Dist. LEXIS 97930 (2007).

purchase histories, social security number and so on. Therefore the Court concluded that "the harm related to disclosure of confidential information in a student or faculty member's internet files [could] be equally harmful" as the damages suffered by Capitol[417].

The ease with which someone might obtain users' identities through the DMCA subpoena has raised the question this could constitute an illegal search and seizure. This is directly linked with the above-mentioned Fourth Amendment insofar as it concerns privacy[418]. "[T]he need for particularity and reliability required by the Fourth Amendment", as specified in case law, is not respected[419].

Moreover, as already said, since the RIAA relied on bots as a monitoring device[420], it has been argued that some people's identities have been wrongly discovered. This means that innocent people have been, and still can be, exposed and can lose their anonymity. This would violate their right to anonymous online speech[421].

The suit by the RIAA would not be the first raising these problems in case of intellectual property enforcement. In 1999 the District Court of Northern California introduced a balancing test in a case of trademark infringement on the Web[422]. Since the plaintiff was not able to identify the defendants, the suit started against "Does". The Does had allegedly registered a domain name, infringing plaintiff's trademark[423]. Similar to what happens in the RIAA cases, in this suit the District Court had to consider whether to uncover the identities of the defendants. The Court ruled that four limiting principles should be screened in deciding about such discovery:

---

417 *Capitol Records, Inc. v. Does 1-16*, cit., 2-3.

418 AMEDEO, *Shifting the Burden: the Unconstitutionality of Section 512(h) of the Digital Millennium Copyright Act and its Impact on Internet Service Providers*, cit., 320.

419 AMEDEO, *Shifting the Burden: the Unconstitutionality of Section 512(h) of the Digital Millennium Copyright Act and its Impact on Internet Service Providers*, cit., 321, refers to *Berger v. New York*, 388 U.S. 41, 56 (1967).

420 As said bots are software tools used by copyright owners to monitor the Internet and detect unauthorized distribution of copyrighted material [*Verizon I*, 38]; they often rely only on terms in the title, which can be misleading.

421 See also AMEDEO, *Shifting the Burden: the Unconstitutionality of Section 512(h) of the Digital Millennium Copyright Act and its Impact on Internet Service Providers*, cit., 321.

422 *Seescandy.com*, 578-80. Apparently this was the first case that considered the difficulties of identifying online users, see N. GLEICHER, *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 Yale L. J. 320, 339 (2008).

423 Columbia is the assignee of numerous trademarks linked to See's Candy Shops, Inc., see *Seescandy.com*, 575. The domain name registered by the defendant was precisely Seescandy.com.

1. "the plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court";

2. "the party should identify all previous steps taken to locate the elusive defendant. This element is aimed at ensuring that plaintiffs make a good faith effort to comply with the requirements of service of process and specifically identifying defendants";

3. "plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss";

4. "the plaintiff should file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible"[424].

Accordingly the Court gave some time to the plaintiff trademark holder for complying with the requirements needed for the discovery[425].

Some "Does" have tried to quash subpoenas also on the basis of privacy concerns[426]. In some cases, courts have shifted the attention to the relation between the ISP and the user. Defendant users could have an expectation of privacy related to their identity[427], but this would depend on the terms of the internet service agreement they had with the Service Provider. This approach was taken, in particular, in *Sony Music Entertainment, Inc. v. Does 1-40*[428]. The District Court, relying on other

[424] *Seescandy.com*, 578-580.
[425] *Seescandy.com*, 581.
[426] Privacy is often connected to the Fourth Amendment, see *supra* and *infra*.
[427] As mentioned, in the seminal case *Katz v. United States*, 389 U.S. 347 (1967) [*Katz*] the Supreme Court announced a new test to be used when coping with Fourth Amendment. In particular, a concurring opinion held in favor of a test that could determine the defendant expectation of privacy; Justice Harlan wrote that the rule needed two different requirements: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'", see *Katz*, 361.
[428] *Sony Music Entertainment, Inc. v. Does 1-40*, 326 F. Supp. 2d 556 (S.D.N.Y. 2004) [*Sony Music Entertainment*]. Followed by *London-Sire Records, INC., et al., v. DOE 1 et al*., 542 F. Supp. 2d 153, 158. (S.D.N.Y. 2009).

courts' earlier decisions, elaborated a sort of "balancing test" to decide whether a subpoena seeking disclosure of users' identities had to be quashed or not[429].

The plaintiffs were seventeen record companies and owners of copyright and exclusive licenses to various songs. They alleged that the forty Does downloaded, distributed or made available for distribution thousands of copyrighted records[430]. The Does, along with their "amici"[431], argued that the discovery violated the First Amendment. Defendants' motion to quash raised essentially two questions on the First Amendment: a) does a person using the internet for music file-sharing engage in a free speech activity?[432] and b) if so, is this person's identity protected from disclosure by the First Amendment?[433]

First, Judge Chin wrote that the Supreme Court recognized that the First Amendment protects anonymous speech also on the internet[434], which is "a particularly effective forum for the dissemination of anonymous speech"[435]. However, anonymous speech is not protected in a total and absolute way. In particular, courts have stated that First Amendment protection of anonymous speech does not protect copyright violation[436]. Nevertheless some courts held that civil subpoenas searching for information of anonymous people may raise First Amendment issues[437]. More recently, courts have faced the problem of subpoenas

[429] *Sony Music Entertainment*, 565.
[430] *Sony Music Entertainment*, 558.
[431] Electronic Frontier Foundation, Public Citizen, and the American Civil Liberties Union (ACLU). Public Citizen is a non-profit, consumer rights advocacy group, see http://www.citizen.org/Page.aspx?pid=2306; ACLU is a non-profit organization "working daily in courts, legislatures and communities to defend and preserve the individual rights and liberties that the Constitution and laws of the United States guarantee everyone in this country", see http://www.aclu.org/about-aclu-0.
[432] The first important decisions taken by the Supreme Court on First Amendment regarded anonymous political speech. Authors and Courts usually agree that anonymous political speech requests the highest level of protection, but they have often raised doubt on whether the same protection should be given to other kinds of speech, see V. SMITH EKSTRAND, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 Comm. L. & Pol'y 405, 413 fn. 40 (2003); see *Sony Music Entertainment*, 564.
[433] *Sony Music Entertainment*, 562.
[434] *Reno v. ACLU,* cit., 870; see also what already said for *Verizon II* and *Verizon Appeal*.
[435] *Sony Music Entertainment*, 562.
[436] *Harper & Row Publishers, Inc. v. Nation Enters.,* 471 U.S. 539, 555-60 (1985).
[437] *Los Angeles Memorial Coliseum Comm'n v. Nat'l Football League,* 89 F.R.D. 489, 494-95 (C.D. Cal. 1981) (granting motion to quash civil subpoena seeking disclosure of confidential journalistic sources).

seeking information from ISPs. As already seen, some of them have granted the subpoena[438], while some others have quashed them[439].

Judge Chin then considered whether music file-sharing could be thought as an exercise of free speech[440]. Ultimately the District Judge held that, even if file-sharing can be considered as a way for expressing ourselves and, therefore, enjoys some First Amendment protection, this protection is limited[441]. Given this statement, the Court analyzed other factors necessary in order to understand whether the identities of anonymous file sharers ought to be protected from disclosure. Judge Chin extracted these factors from previous decisions, including:

1) concrete showing of a prima facie claim of actionable harm;
2) specificity of the discovery request;
3) absence of alternative means to obtain the subpoenaed information;
4) central need for the subpoenaed information to advance the claim; and
5) the party's expectation of privacy[442].

The actual showing of prima facie claim of copyright infringement is supported by demonstrating ownership of a valid copyright and the copying of constituent elements of the copyrighted work that are original. In this case the recording companies had brought a list of the recordings allegedly downloaded by the Does. Then the plaintiffs demonstrated that those songs came along with a valid Certificate of Copyright Registration and that among their exclusive rights are those to reproduce and distribute to the public. Furthermore, the plaintiff recording companies had alleged that, without their consent, defendants used a file-sharing system to download, distribute or make available to others these copyrighted

---

438 *Verizon I* and *Verizon II*; *In re Subpoena Duces Tecum to America Online, Inc.,* cit.

439 *Verizon Appeal*; *Doe v. 2TheMart.Com,* 140 F. Supp. 2d 1088, 1097-98 (WD Wash. 2001).

440 DICKMAN, *Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits*, cit., 1066 argues that when a user downloads and makes available to others music she likes, she is unquestionably exercising her free speech right coming directly from First Amendment. Prof. Julie Cohen which claims that freedom of reading anonymously is an expression of identity. Readers would have a legitimate interest in not disclosing information related to her preferences, interests and beliefs [cf. J. COHEN*, A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 Conn. Law Review 981 (1996), spec. 1012-1013]. See also the decision *Tattered Cover, Inc. v City of Thornton*, 44 P.3d 1044, 1047 (Colo. 2002), on the right to anonymously purchase books. We could probably assimilate this vision to the listening of music. The idea of Dickman, however, goes a bit further.

441 *Sony Music Entertainment*, 564. Followed by *UMG Recording, Inc. v. Does 1-4*, 2006 U.S. Dist. LEXIS 32821, 5 (N.D. Cal. 2006); *Elektra Entertainment Group, Inc. v. Does 1-9*, 2004 U.S. Dist. LEXIS 23560, 8 (S.D.N.Y. 2004).

442 *Sony Music Entertainment*, 564-565.

songs[443]. Judge Chin noted that the use of a P2P network to share files over the internet had already been held as copyright infringement[444]. Therefore, the record companies had sufficiently proven copyright infringement to establish a prima facie claim[445].

As far as the second requirement is concerned, plaintiffs had made a sufficiently specific discovery request to determine that the discovery would likely lead to identifying information of persons that could be sued in federal court. Plaintiffs based their request on given times and date when the Does downloaded specific copyrighted songs. The companies then proved that they had no other means than the subpoena to obtain users' identities and that this information was fundamental in order to carry out their claims[446].

Finally Judge Chin dealt with the question of defendants' expectation of privacy. According to his opinion, the defendant users could have had only a minimal expectation of privacy. The terms of service of their contract with the ISP specifically stated that the transmission or distribution of material in violation of any law or regulation, including copyrighted works without proper authorizations, was prohibited[447]. The same terms further stated that the ISP had the right to disclose any information necessary to satisfy any law, regulation or other governmental request[448]. As a result of this analysis, the Court decided that the plaintiffs' right to pursue copyright infringement claims outweighed defendants' right of anonymity[449].

Even if the holding made by this Court is more wide-ranging than privacy/first amendment issues, it is interesting to note as a practical matter the manner which the Court attempted to balance copyright owner's rights with users'

---

443 *Sony Music Entertainment*, 565. Defendants failed to refute plaintiffs' allegation of ownership, *Ibidem*.

444 The District Court refers first of all to *Napster Appeal*, 1013-14.

445 *Sony Music Entertainment*, 565-566.

446 *Sony Music Entertainment*, 566.

447 The ISP was Cablevision System Corporation, which is "a leading telecommunications, media and entertainment company with a portfolio of operations that includes a full suite of advanced digital television, voice and high-speed Internet services, some of the country's most-watched national television networks, and valuable local media and programming properties", see http://www.cablevision.com/about/index.jsp.

448 See Terms of Service for the high-speed Internet access at http://www.optimum.net/Terms. For this fifth step Judge Chin also referred to *Verizon II* at 260-261, 267-268, where the District Court argued that when an individual opens her computer to other people through P2P file-sharing, she cannot expect to enjoy privacy. *Sony Music Entertainment* reasoning about privacy expectation was followed in *Doe I v. Individuals*, 561 F. Supp. 2d 249, 255 (D. Conn. 2008).

449 *Sony Music Entertainment*, 567.

rights. Judge Chin's evaluation is only one of many other "balancing acts" that courts have used to decide whether or not unmask an anonymous user. As stated, First Amendment protects the right to speak anonymously. Many courts have felt the need for a balancing between defendant's rights to anonymity and plaintiff's rights to seek redress over violation of a property or property-like right. More and more lawsuits are involving anonymous internet "speakers". This raises a new problem for courts, especially in the phase of unmasking such interlocuteurs[450]. Allowing plaintiffs to easily unmask anonymous speakers could create a chilling effect on free speech.

With the increasing use of the internet, it is also true that the number of lawsuits involving anonymous users has grown[451]. In the beginning, courts were not very worried about First Amendment issues and let plaintiffs proceed with little or no discussion[452]. Then they started to show a greater sensitivity to speech and privacy issues, and subsequently to feel the need for a balance. Courts defined different standards for revealing real identities or specific criteria that parties should meet when seeking to identify anonymous people[453]. Summarizing, these standards normally require that parties seeking the identities of anonymous speaker demonstrate:

a) that they made reasonable attempts to provide notice of the subpoena to the anonymous speakers[454], typically an adequate notice and reasonable opportunity to respond;

---

[450] M. MAZZOTTA, *Balancing Act: Finding Consensus On Standards For Unmasking Anonymous Internet Speakers*, 51 Boston College L.R. 833, 839 ff. (2010).

[451] See L. BARNETT LIDSKY, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 Duke L.J. 855 (2000) describing the tactics used by big companies to sue anonymous users who posted defamatory messages on web boards.

[452] See for example *In re Subpoena Duces Tecum to America Online, Inc*., cit.

[453] L. BARNETT LIDSKY, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 Boston College L.R. 1373, 1376 (2009). See also MAZZOTTA, *Balancing Act: Finding Consensus On Standards For Unmasking Anonymous Internet Speakers*, cit., 866 ff. This author made a survey among ten different unmasking standards, underling convergences and divergences within them. Many other scholars have similarly contributed to the discussion on identity disclosure in case of First Amendment issues and the need for a standard "unmasking test", among the most recent: SMITH EKSTRAND, *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, cit., 417 ff.; GLEICHER, *John Doe Subpoenas: Toward a Consistent Legal Standard*, cit., 338 ff.; C. CALVERT, K. GUTIERREZ, K.D. KENNEDY, K. CARNLEY MURRHEE, *David Doe v. Goliath, Inc.: Judicial Ferment in 2009 for Business Plaintiffs* Seeking *the Identities of Anonymous Online Speakers*, 43 J. Marshall L. Rev. 1 (2009), spec. 41 ff, where the authors compare the tests used by different course between 2008 and 2009; J.D. JONES, *Cybersmears and John Doe: How Far Should First Amendment Protection of Anonymous Internet Speakers Extend?*, 7 First Amend. L. Rev. 421 (2009).

[454] This is often a problem when the subpoenaed party is an ISP: they sometimes do not contest the subpoenas nor notify anonymous speakers about them; see MAZZOTTA, *Balancing Act: Finding*

b) that there is some evidence on the merits of the claim[455]; and

c) that it has a real need for the identifying information[456].

Some courts then consider an additional "First Amendment balancing prong" to fully protect the user's right to (anonymous) free speech and some measure of privacy. The first court which applied this additional requirement was the Superior Court of New Jersey[457]. The Court stated that the application of a "motion-to-dismiss standard in isolation fail[ed] to provide a basis for an analysis and balancing of Dendrite's request for disclosure in light of John Doe No. 3's competing right of anonymity in the exercise of his right of free speech"[458]. Even if in the end the Court did not really supply a rule for resolving the conflict, it underlined the necessity of a "flexible, non-technical, fact-sensitive mechanism" as a warranty against discovery abuses[459].

So, on one side of the balance is placed the plaintiff's need for the identifying information and on the other side is placed the defendant's right to anonymity. According to what we have said so far, judges should in first place value plaintiff's needs. Only after that, they should move to First Amendment rights. This second step can sometimes be really important, since unmasking requests can arise from very

---

Consensus On Standards For Unmasking Anonymous Internet Speakers, cit.,843. When the identity of the defendant is unknown, this requirement cannot be applied too strictly. This is why courts have sometimes held that posting notice of the suit in the forum where Doe posted his allegedly defamatory statement was sufficient; see for example *Doe v. Cahill*, 884 A.2d 451, 461 (Del. Supr. 2005).

[455] According to Barnett Lidksy courts' tests normally comes down only to these two elements. This second requirement has been thought in different ways: a) as a showing that the claim was brought in good faith; b) as a showing that the claim could withstand a motion to dismiss; c) as a showing that the claim could withstand a motion for summary judgment; d) as a showing of prima facie evidence for all elements of the claim, see MAZZOTTA, *Balancing Act: Finding Consensus On Standards For Unmasking Anonymous Internet Speakers*, cit., 850-851 and BARNETT LIDSKY, *Anonymity in Cyberspace*, cit., 1378, who asserts that d) is the dominant standard.

[456] Need-based inquiries have been defined in different ways as well, investigating whether there were other means of obtaining information or the scope of the identifying request, or whether the information sought was relevant or otherwise important for the lawsuit, and so on; see MAZZOTTA, 854.

[457] *Dendrite International, Inc. v. Doe, no. 3*, 775 A.2d 756 (NJ Super. 2001); the standard used in this case seems to be "gaining ground as the dominant standard", BARNETT LIDSKY, *Anonymity in Cyberspace*, 1378; according to FROOMKIN, *Anonymity and the Law in the United States*, cit., 454 "[m]any states now use some version of the so-called *Dendrite* principles".

[458] *Ibidem*, 770.

[459] Other courts then provided for other balancing prongs for the First Amendment, see MAZZOTTA, *Balancing Act: Finding Consensus On Standards For Unmasking Anonymous Internet Speakers*, cit., 857 ff. Some courts instead found it unnecessary or too burdensome for the plaintiff, see MAZZOTTA, *Balancing Act: Finding Consensus On Standards For Unmasking Anonymous Internet Speakers*, cit., 858 fn. 170.

different situations[460]. Considering "the content and context of the speech, […] the harm caused by the speech, […] and the potential harms that unmasking would pose to the anonymous speaker" could really help in the hard task of balancing[461]. It is not unusual, indeed, that the context where a violation occurs can be an embarrassing one or even a cause for harassment[462].

The balancing tests used by courts with regard to protecting First Amendment "cyber-speech" is undoubtedly a source of interesting clues for the conflict between the enforcement of copyright and the protection of private data. Nevertheless, in deciding that the ISP shall divulge users' identities, virtually all courts noted that the Supreme Court made it clear that the First Amendment cannot cover copyright infringement[463], so the degree of anonymity protection is considered minimal when coping with copyright infringement[464].

The problem goes back to the question of "which kind of rights in conflict?". In the analyzed First Amendment cases usually there is a plaintiff's right to obtain

---

[460] Authors do not always agree on this. BARNETT LIDSKY, *Anonymity in Cyberspace*, cit., 1380 argues that as long as under the prima facie evidence standard the plaintiff presents evidence that the claim is viable, this outweighs the defendant's right to speak anonymously. She thinks that the use of a separate balancing test would increase the protection of anonymous speech, since more claims would be dismissed on the ground that they are not strong enough compared to First Amendment issue. The author proposes that the court consider *in camera* the defendant's actual reason for speaking anonymously before deciding on the disclosure, BARNETT LIDSKY, *Anonymity in Cyberspace*, cit., 1380 fn. 40; see also L. BARNETT LIDSKY, T. COTTER, *Authorship, Ardencies, and Anonymous Speech*, 82 Notre Dame L. Rev. 1537, spec. 1601 ff. (2007).

[461] MAZZOTTA, *Balancing Act: Finding Consensus On Standards For Unmasking Anonymous Internet Speakers*, cit., 864. "[W]ithout a balancing step, the superior court would not be able to consider factors such as the type of speech involved, the speaker's expectation of privacy, the potential consequence of a discovery order to the speaker and others similarly situated, the need for the identity of the speaker to advance the requesting party's position, and the availability of alternative discovery methods. Requiring the court to consider and weigh these factors, and a myriad of other potential factors, would provide the court with the flexibility needed to ensure a proper balance is reached between the parties' competing interests on a case-by-case basis", see *Mobilisa v. Doe*, 170 P.3d 712, 720 (Ariz. Ct. App. 2007).

[462] Let us suppose that Jane Doe is a lesbian, who shares adult movies according to her sexual orientation. Let us further suppose that she has never outed her homosexuality. If her name was discovered, she may be subject to harassment, which is exactly what she tried to avoid when decided to keep her sexual orientation secret.

[463] *Verizon II*, 260, quoting *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 220 (S.D.N.Y. 2000); *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 568 (1985); *Zacchini v. Scripps-Howard*, 433 U.S. 562, 574-78 (1977). "[T]he First Amendment is not a license to trammel on legally recognized rights in intellectual property", see *In re Capital Cities/ABC, Inc.*, 918 F.2d 140, 143 (11th Cir. 1990).

[464] *Verizon II*, 260. The idea of using a balancing test in copyright infringement John Doe cases has been criticized, since DMCA subpoena requirements would equal the described tests applied by courts, see RAYNOLDS, *One Verizon, Two Verizon, Three Verizon, More? – A Comment: RIAA v. Verizon and How The DMCA Subpoena Power Became Powerless*, cit., 369-370 ff. See also *Verizon II*, 264, fn. 22.

redress for libel or defamation or harassment and a defendant's right to remain anonymous, given that what she said was part of her First Amendment right to free speech. In cases like *Verizon,* we have the RIAA (or similar copyright-holder entities) trying to enforce economic (copy)rights of its associates against Does who try to preserve their constitutional right to privacy. Then the problem goes back again to privacy: is it really a constitutional right? Since there is no specific constitutional right to privacy, "the Supreme Court has developed a limited, "penumbral" conception of this right flowing from a variety of constitutional sources - the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments"[465].

Might it simply be a matter of social consensus or an evolving social norm? Somebody sharply wrote that "the Internet has not been a part of American culture for long enough to determine the impact of the potential First Amendment infringement that ISP compliance with the DMCA might occasion"[466]. Could the same be said about privacy and personal data protection? Certainly the recent trends, across many jurisdictions including the USA, to value and protect privacy and information privacy is indicative of an increasingly importance given to this topic.

[465] KATYAL, *Privacy v. Piracy*, cit., 238 fn. 45 (2004).

[466] A.R. FOX, *The Digital Millennium Copyright Act: Disabusing the Notion of a Constitutional Moment*, 27 Rutgers Computer & Tech. L.J. 267, 287 (2001). The Author compares the DMCA approval with other "constitutional" moments of American history. He concludes that DMCA could have been an important moment, a consciousness raising of public at large, but it did not because of the above stated reason.

Chapter 3
The Canadian System

3.1 The legal framework of file sharing

Contrary to what happens for personal data legislation and privacy protection, in Canada copyright is a subject on which only the federal lawmaker can legislate[1]. The current *Copyright Act* was enacted in 1921 and it is the sole copyright legislation applicable, even if it has been frequently and substantially amended since its appearance[2]. The Act states that no copyright or other rights should exist in Canada other than under the *Copyright Act* itself[3].

When the Act was enacted, it applied only to published manuscripts. Nowadays, it obviously protects a host of works, including music, architectural plans, computer programs and also unpublished works. In particular, it grants copyright to "every original literary, dramatic, musical and artistic work" upon the creation of the work[4]. Automatic protection of copyright is not affected by the possibility to register the work. Registration is indeed unnecessary for the subsistence of copyright, but there are some procedural advantages for the copyright owner whose work is registered. More precisely, as in the US, one of the advantages of registration is that the certificate of registration would constitute evidence that copyright exists in that work and that the person registered is the owner of the rights. In other terms, it would be a *prima facie* evidence of copyright ownership[5].

The *Act* protects also the so-called "neighbouring rights", which are rights related to the performance, recording or broadcasting of a work. To enhance the protection of these rights, a substantial change in the *Act* was made in 1997 to

[1] This is by virtue of Section 91(23) of the Constitution Act of 1867. This Act, formerly known as the British North America Act (BNA Act), is a major part of the Canadian Constitution. Cf. P.W. HOGG, *Constitutional Law of Canada*, Toronto, 2010, 1-7 ff. From this point of view the USA and Canada have the same kind of federal regime.
[2] *Copyright Act*, R.S.C., 1985, c. C-42. For an account of the reforms occurred in the Canadian landscape of copyright see J.S. MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, Scarborough, 2000, 39 ff..
[3] S. HANDA, *Copyright Law in Canada*, Markham, 2002, 55.
[4] *Copyright Act*, s. 5(1).
[5] MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, cit., 403 ff.

include and expand them[6]. However, *les droits voisins* are protected in a rather different way from those related to the traditional works, for example, with regard to the terms of protection[7].

As already stated, nowadays the *Copyright Act* also protects music[8]. In particular a "musical work" is defined as "any work of music or musical composition, with or without words and includes any compilation thereof"[9]. The sentence "with or without words" was inserted with a subsequent amendment, in effect after 1993, in order to include songs under this section's protection[10]. The earlier definition could apply only to musical works in their printed or graphic form, but not to the acoustic presentation of the work[11]. Musical recordings are protected separately under neighbouring rights. Thus, there are various "layers" of copyright protection in a larger musical work: the music as written, the lyrics, the lyrics and music together as the song, the sound recording, and, as we shall see, any performance and broadcasting rights associated with that "song".

Neighbouring rights are divided into performers' rights, the rights of sound recording makers and the rights of broadcasters. Performance is "any acoustic or visual representation of a work, performer's performance, sound recording or communication signal, including a representation made by means of any mechanical instrument, radio receiving set or television receiving set". Furthermore there is a "performer's performance", which can be:

[6] The changes were first proposed by Bill C-32, *An Act to amend the Copyright Act*, S.C. 1997, c. 24, s. 6.
[7] HANDA, *Copyright Law in Canada*, cit., 143.
[8] For a brief history of the protection of musical and dramatic works starting from the Statute of Anne, see MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, cit., 188 ff.
[9] *Copyright Act*, s. 2. As to the cinematographic works, the Act included them in dramatic works and comprises also works "expressed by any process analogous to cinematography, whether or not accompanied by a soundtrack". *Copyright Act*, s. 2: "dramatic work" includes (*a*) any piece for recitation, choreographic work or mime, the scenic arrangement or acting form of which is fixed in writing or otherwise, (*b*) any cinematographic work, and (*c*) any compilation of dramatic works". Despite the fact that some of the lawsuits brought in front of courts against P2P related to movies, I shall concentrate on musical works.
[10] The previous definition included "any combination of melody and harmony, or either of them, printed, reduced to writing or otherwise graphically produced or reproduced", cf. D. VAVER, *Copyright Law*, Toronto, 2000, 47; MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, cit., 188.
[11] MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, cit., 465.

a. "a performance of an artistic work, dramatic work or musical work, whether or not the work was previously fixed in any material form, and whether or not the work's term of copyright protection under this Act has expired,
b. a recitation or reading of a literary work, whether or not the work's term of copyright protection under this Act has expired, or
c. an improvisation of a dramatic work, musical work or literary work, whether or not the improvised work is based on a pre-existing work"[12].

The Act does not provide a definition for "performer", but it describes three main performer's sole rights. When the work is not fixed in a tangible form, the performer has the right to: 1. communicate it to the public by telecommunication; 2. perform it in public, where it is communicated to the public by telecommunication different from a communication signal; 3. fix it in any material form. Whenever the work is already fixed, the performer can: 1. reproduce any fixation that was made without the performer's authorization; 2. where the performer authorized a fixation, reproduce any reproduction of that fixation, if the reproduction being reproduced was made for a purpose other than that for which the performer's authorization was given; 3. where a fixation was permitted as an exception to infringement or for private use, reproduce any reproduction of that fixation, if the reproduction being reproduced was made for a purpose other than one permitted under the exception to infringement or for private use. In any case, the performer has the right to rent out a sound recording of the performance and to authorize any of the above listed acts[13].

With relation to "sound recording" the Act defines it as "a recording, fixed in any material form, consisting of sounds, whether or not of a performance of a work, but excludes any soundtrack of a cinematographic work where it accompanies the cinematographic work"[14]. Section 18 of the Act provides that the maker of a sound recording has a sole right related to the sound recording or to any substantial part of it to publish it for the first time, to reproduce it in any material form, and to rent it out. It includes also the right to authorize any of these actions[15].

[12] *Copyright Act*, s. 2.
[13] *Copyright Act*, s. 15(1)(a)-(c); see HANDA, *Copyright Law in Canada*, cit., 182 ff. These rights are limited by s. 15(2).
[14] *Copyright Act*, s. 2.
[15] *Copyright Act*, s. 18(1). There rights are conditional on the existence of certain factors listed in section 18(2).

All the above-mentioned rights terminate 50 years after the end of the calendar year in which a performer's performance is first fixed in a sound recording, or its performance, if it is not fixed in a sound recording[16].

As said, the *Copyright Act* sets out a closed list of rights. No other rights, for example common law rights, are applicable. This has been affirmed in a number of important cases. In particular Section 3(1) defines what constitutes copyright in a work and gives a list of economic rights. Copyright is therefore "the sole right to produce or reproduce the work or any substantial part thereof in any material form whatever, to perform the work or any substantial part thereof in public or, if the work is unpublished, to publish the work or any substantial part thereof"[17]. Copyright includes other rights, as for example, to produce, reproduce, perform or publish a translation of the copyrighted work; or in case of a literary work, the right to reproduce, adapt and publicly present it as a cinematographic work. In any case the copyright owner has the right to authorize such acts[18].

Regarding the three "main" rights are concerned, they can be summarized as follows:

- to produce or reproduce: as courts have clarified, to produce a work means bringing it to existence[19]. Reproduction is not defined by the Act either, but it has been used as a synonym for the notion of copying[20], and that new copies must be created in order to have reproduction. This right is limited to the entire work or any substantial part of it; to define whether the reproduction made was substantial, all the circumstances of the case must be taken into account. In this regard, a clue can be offered, for example, by the quality and quantity of the material taken (in that order, with quality taking precedence over quantity), including the importance of the parts taken or the purpose for which the material was taken and the economic impact on the market for the plaintiff's work[21];

[16] *Copyright Act*, s. 23(1).
[17] *Copyright Act*, s. 3(1).
[18] *Copyright Act*, s. 3(1)(a)-(i).
[19] *Compo Co. v. Blue Crest Music Inc.*, [1980] 1. S.C.R. 357, par. 32.
[20] HANDA, *Copyright Law in Canada*, cit.,196, citing *Hanfstaengl v. Empire Palace*, [1894] 2 Ch. 1.
[21] For an overview of the different indications taken into account by courts in deciding whether the reproduction was of a substantial part or not, see MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, cit., 424 ff.

- to perform: first of all it should be noted that this right differs from that granted to the performer under Section 15. A performance has been defined as an act that causes the work to be heard or seen[22]. Subsection 3(1 only grants a copyright holder the sole right to perform a work, when the performance is carried out in public[23]. As to the meaning of "public", it is important to remark that, despite the transmission of a musical work by electronic signals through telephone cables has been considered as a public performance[24], the same cannot be said about the watching of a work in one's private home through cable television or Internet. But it could constitute public performance if the watching was made in a public place[25]. This right is separate and distinct from the traditional idea of reproduction and exists side by side with the latter one[26];
- to publish: it is the right to publish an unpublished work; it lasts until its first publication. Whenever a work is made available for sale by the author, the exclusive right to offer it for sale will be exhausted and anyone may sell the work[27]. A work cannot be said to be published if the communication to the public occurred without the consent of the owner of the copyright[28].

Following what I have written so far, a recorded musical work, such as a song, would enjoy the protection of multiple sections. Therefore, the copying of a song can potentially infringe several aspects of copyright[29]. This could be the case in peer-to-peer file sharing. Nevertheless, in Canada, up to now, file sharing for music does not seem to be clearly illegal. That is, there are doubts as to the legality or illegality of such an activity. The reasons for these doubts are found in s. 80 of the Copyright Act., and in that the current position of Canadian law (after the Tariff 22 case) is that "making available" does not constitute copyright infringement.[30]

Section 80(1) of the *Copyright Act* provides a specific exception to infringement related to sound recordings, which is the so-called "private copying"

[22] *Canadian Admiral Corp. v. Rediffusion Inc.*, [1954] Ex. C.R. 382, par. 62.
[23] See supra Section 3(1).
[24] *Associated Broadcasting Co. et al. v. Composers, Authors, and Publishers Association of Canada Ltd*, [1954] 3 All E.R. 708, cited by HANDA, *Copyright Law in Canada*, cit.,198.
[25] *Canadian Cable Television Assn. v. Canada (Copyright Board)*, 34 C.P.R. (3d) 521, par. 30.
[26] MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, cit., 190.
[27] HANDA, *Copyright Law in Canada*, cit., 199.
[28] *Copyright Act*, s. 2.2(3).
[29] Clearly, the same could e said for a cinematographic work.
[30] Tariff 22, etc.

exception. This exception provides that reproducing all or a substantial part of a musical work onto an "audio recording medium" (like an audio cassette tape) for the private use of the person who makes the copy does not constitute infringement. The provision has itself some limitations. It cannot be applied to those who copy music with the aim of selling, renting out, distributing, communicating to the public by telecommunication or performing the work in public[31]. Furthermore, the Section exonerates from liability only those who records music, but not those who record other kind of works, such as a comedy. Finally, the question of what constitutes an "audio recording medium" is ambiguous, and a computer may not necessarily provide a platform for the exception[32].

This section was added in 1997, as a response to the ceaseless complaints of the music industry for the alleged decline in record sales that would have been due to the unauthorized home copying of sound recordings[33]. In order to compensate copyright holders for the losses they could incur as a result of the introduction of this section, the Act introduced a levy to be paid by the manufacturers and importers of blank audio recording media to a collecting body[34]. The levy revenues are divided between authors, performers and record makers[35]. Levies are filed by collective societies[36] with the Copyright Board of Canada[37].

The Copyright Board of Canada, established in 1936 with the name of Copyright Appeal Board, is an economic regulatory body, which core function is considering the statements of fees and royalties that performing rights societies

[31] *Copyright Act*, s. 80(1) – *Where no infringement of copyright* – and s. 80(2) – *Limitations*.
[32] See Gervais & Judge. Based on FCA cases. I don't agree with Gervais here.
[33] VAVER, *Copyright Law*, cit., 223.
[34] One of these collective societies is the Society of Composers, Authors and Music Publishers of Canada (SOCAN), for which see below.
[35] See the Copyright Board's decision *Private Copying*, 18 December 1999, which can be found at http://www.cb-cda.gc.ca/decisions/1999/19991217-c-b.pdf. Cf. also *Copyright Act*, s. 84. Some commentators claim that levies would yet be the best solution to P2P, see for example NETANEL, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, cit.
[36] For an overview of the Canadian collective societies, see D.J. GERVAIS, *A Uniquely Canadian Institution: the Copyright Board of Canada*, in Y. GENDREAU (ed.), *Emerging Intellectual Property Paradigm: Perspectives from Canada*, Cheltenham, 2008, 199 ff.
[37] *Copyright Act*, s. 81(1) ff. The procedure is as follows: every year before the 31st of March a proposed tariff is filed by a collective society; the tariff is published by the Board in the *Canada Gazette* and users, also through their representatives, can object within 60 days. The Board then sets a timetable for the proceedings; collectives and users representatives can argue their case before a panel of three judges. After deliberation, the Board certifies the tariff, which is published again in the *Canada Gazette* and provides for its reasons. The tariff becomes effective on the 1st of January of the following year. Cf. GERVAIS, *A Uniquely Canadian Institution: the Copyright Board of Canada*, cit., 210-211.

proposed to charge. The Board has also the power and the right to supervise agreements between users and licensing bodies, and it issues licences when copyright owner cannot be located[38]. Finally, the Board possesses jurisdiction above the mentioned matters, as it is an independent administrative tribunal[39].

Section 80(1) has proven to be very important for file-sharers in Canada. In fact, as mentioned, the interpretation of this section, together with other elements, has led to the conclusion that file sharing of music files in Canada is not illegal, or at least that the illegality of file-sharing of music files is questionable. This interpretation is supported by three main decisions: *BMG Canada Inc. v. John Doe* by the Federal Court[40]; *CCH v. Law Society of Upper Canada* by the Supreme Court[41] and the *Private Copying 2003-2004* decision by the Copyright Board[42].

In December 2003, the Copyright Board, solving some issues related to the exemption for private copying, stated: "[t]he [*private copying*] regime does not address the source of the material copied. There is no requirement […] that the source copy be a non-infringing copy. Hence, it is not relevant whether the source of the track is a pre-owned recording, a borrowed CD, or a track downloaded from the Internet". Moreover the Board added that "[a]lthough the source of the copy does not matter, the destination does. The Board believes that section 80 creates an exemption

[38] Cf. the Board's website at http://www.cb-cda.gc.ca/about-apropos/mandate-mandat-e.html. See also MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, cit., 692; HANDA, *Copyright Law in Canada*, cit.,141. The activities and responsibilities of the Board are regulated by the *Copyright Act*, s. 66(1) ff.

[39] GERVAIS, *A Uniquely Canadian Institution: the Copyright Board of Canada*, cit., 210. Decision made by the Copyright Board do not have a statutory right of appeal. Indeed, a person should make an application for judicial review before the Federal Court of Appeal, cf. HANDA, *Copyright Law in Canada*, cit.,355. Copyright infringement cases can be brought either in front of the Federal Court of in a provincial Superior Court, since both have jurisdiction on this matter. When the issue is related only to copyright, the case will typically be issued in front of the Federal Court, given that it has more expertise on intellectual property, cf. *Ibidem*,141. The Federal Court of Canada and the Federal Court of Appeal (like the Supreme Court) were created by statute by the federal government for the "better Administration of the Laws of Canada". They were intended to have jurisdiction only on those matters where the federal government had made laws, that is "applicable and existing federal law". Through the Federal Court Act the jurisdiction of the Federal Courts was modified and now one of the most important areas in which the courts decide is intellectual property law. The two courts are now two distinct administered courts, and ceased to be one court with a trial and an appellate division. Cf. J. WALKER, L. SOSSIN, *Civil Litigation*, Toronto, 2010, 167, 13-14; L.S. ABRAMS, K.P. MCGUINNES, *Canadian Civil Procedure Law*, Markham, 2010, 50-52. See also HOGG, *Constitutional Law of Canada*, cit., 7-26 ff.

[40] *BMG Canada Inc. v. John Doe*, [2004] 3 F.C.R. 241 [*BMG I*]. See below for a detailed analysis.

[41] *CCH Canadian Ltd. v. Law Society of Upper Canada*, [2004] S.C.R. 339 [*CCH*]. See later in this chapter for a summary.

[42] *Private Copying 2003-2004*, December 12, 2003, available at: http://www.cb-cda.gc.ca/decisions/2003/20031212-c-b.pdf [*Private Copying 2003-2004*]

that applies as long as two conditions are met: the copy must be for the private use of the person making it, and it must be made onto an audio recording medium, as defined in section 79"[43]. Taking this position, the Board stated that – at least – the downloader could not be considered an infringer.

In *BMG*, relying in part on the Copyright Board's reasoning mentioned above, the Federal Court held that "downloading a song for personal use does not amount to infringement"[44]. Referring to *CCH*, the Federal Court claimed that there had not been any distribution or authorized reproduction of sound recordings. *CCH*, indeed, stated that to have a secondary liability infringer, she has to "authorize" the illegal activity of the primary infringer. Given the fact that a file-sharer put in her computer files that can be downloaded without her knowledge or even without her permission by other peers[45], there was no evidence that the alleged infringer distributed or authorized the reproduction of sounds recordings. The Court saw no difference between the CCH case, in which a library put a photocopy machine in a room full of copyrighted material, and the BMG case, in which users placed a *personal copy* of songs on a shared directory of their computers, linked to a P2P. This would not, moreover, account as distribution, for there is no positive act by the owner of the shared directory[46]. Despite the Federal Court of Appeal was not of like mind and clarified that it was premature to reach a conclusion with regard to the legality of P2P file sharing[47], authors and commentators believe that this was a win for P2P legality in Canada[48].

[43] *Private Copying 2003-2004*, 20. Section 79 supplies for the definition of the Part of the Copyright Act related to Private Copying. The Section defines an "audio recording medium" as "a recording medium, regardless of its material form, onto which a sound recording may be reproduced and that is of a kind ordinarily used by individual consumers for that purpose, excluding any prescribed kind of recording medium"; furthermore, the Section defines "blank audio recording medium" as "(a) an audio recording medium onto which no sounds have ever been fixed, and (b) any other prescribed audio recording medium".
[44] *BMG I*, par. 25.
[45] Apparently, some P2P systems place a user's downloaded songs in a shared folder by default, and this passive sharing does not seem enough to be an "authorization" to copyright infringement. Cf. F. TABATABAI, *A Tale of Two Countries: Canada's Response to Peer-to-Peer Crisis and What It Means for the United States*, 73 Fordham Law Review 2321 (2005), 2347.
[46] *BMG I*, par. 26-28, *sic passim*. Emphasis added.
[47] *BMG Canada Inc. v. John Doe*, [2005] F.C.J. No. 858, paras. 46 ff [*BMG II*].
[48] See for example: TABATABAI, *A Tale of Two Countries: Canada's Response to Peer-to-Peer Crisis and What It Means for the United States*, cit., 2343 ff.

CCH reasoning on secondary liability does certainly apply to ISPs and to P2P software producers[49], but for someone this would not be applicable to users, as the Court in BMG would like. Even if it is true that P2P users do not have any duty to supervise their peers, it is not so easy to argue that their role is totally passive[50]. In fact, according to some scholars, the moment in which a P2P user puts in her shared folder a sound recording, she moves from the copy for private use to a distribution and/or communication of the same[51]. Actually, in Canadian copyright "distribution" is not a right of the copyright holder; nevertheless, in case a copy was made for distribution, it would not be covered by Section 80(1) since it is not for private use. Furthermore, unless, as mentioned, the software does this operation on its own, when placing a song in the shared folder a user infringes the "authorization" right.

Besides, section 80(1) considers the copy "onto an *audio recording medium*"; for some authors a personal computer does not constitute a medium within the meaning of the section 80(1). In fact, an audio recording medium is regarded as one that is "ordinarily used" by individuals to record music and on which consumers pay the already mentioned levy. A consumer does not infringe copyright as long as she records on that medium and as long as she records music, for no other forms of copyrighted works are covered by section 80(1). The section does not cover media that are considered not to be ordinarily used to record music; for example consumers do not pay the levy for DVDs, but at the same time they are not allowed to use the private copying exception. Hence, in this case the person would infringe copyright, unless she has the permission to copy from the rights holder[52].

---

[49] Given that these softwares have both infringing and non-infringing uses, see E.F. JUDGE, D.J. GERVAIS, *Intellectual Property: The Law in Canada*, Toronto, 2011, 184.

[50] Actually, "concepts of downloading and uploading are not entirely apt and are used here primarily as a convenient way of categorizing the infringement issues. Strictly speaking, the concepts assume a form of client-server architecture within which "downloading" refers to copying a file onto a client from a server, while "uploading" refers to copying the file onto a server from a client. Within a pure P2P architecture, each client is also a server, so that downloading onto a client is also, simultaneously, uploading onto a server, and *vice-versa*. Hence, *except for an initial uploader* who injects works into the system from a source outside the system, such as a compact disc, every event of uploading is also a download", G.R. HAGEN, N. ENGFIELD, *Canadian Copyright Reform: P2P Sharing, Making Available and the Three-Step Test*, 3 UOLTJ 477 (2006), 485 fn. 34.

[51] JUDGE, GERVAIS, *Intellectual Property: The Law in Canada*, cit., 184; see also D.J. GERVAIS, *Canadian Copyright Law Post-CCH*, 18 Intellectual Property Journal 131 (2004), 150 ff.

[52] JUDGE, GERVAIS, *Intellectual Property: The Law in Canada*, cit., 260. But see *Private Copying 2003-2004*, 21: "[i]t would indeed seem illogical that the scope of the exemption could depend on the rights-holders' unilateral choice to propose or not a tariff. For instance, simply because the Board has not been asked to certify a tariff on hard disks in personal computers, it does not follow that private

Section 79 defines an "audio recording medium" as a "a recording medium, regardless of its material form, onto which a sound recording may be reproduced and that is of a kind ordinarily used by individual consumers for that purpose, excluding any prescribed kind of recording medium". The categorization of a medium as "ordinarily used" for the record of music is quite problematic. Some think that this definition should be thought dynamically: the provision should apply not only to those media which were ordinarily used for that scope at the time of the enactment, but also to those which become ordinarily employed over the time[53]. This is the approach taken, for example, by the Copyright Board[54]. Others propose a case by case approach, in which the "ordinary use" of a product, such us a PC's hard disk, is to be considered as an empirical issue, and not as an *a priori* matter of law[55].

What exactly should be meant for "medium" is under question. For example, in one if its decisions the Copyright Board claimed that it was important to take in consideration the kind of device in which the recording medium was incorporated. This meant that a hard disk would have been a medium under section 79 if embedded in a MP3 player, but not in a personal computer[56]. So, this reading of section 79 could lead to the conclusion that whenever a consumer downloads directly on her computer hard disk, the exception provided by section 80(1) does not apply[57]. The Federal Court of Appeal, in reversing the Copyright Board's decision, claimed that the device was not to be taken into account and ruled that the Board erred in its decision. The Federal Court also acknowledges that the Board had interpreted section 79 in that sense, in order to include MP3 players in the list of media to which the levy should apply[58].

---

copies made onto such media infringe copyright. Moreover, to argue that a private copy on a particular kind of medium is legal only if a levy was paid on that particular unit would be to add a condition that is not currently included in section 80"

[53] JUDGE, GERVAIS, *Intellectual Property: The Law in Canada*, cit., 261.

[54] *Private Copying 2003-2004*, 43. This interpretation of section 79 creates a dilemma: what about new media in the phase where they are not yet ordinarily used for music recordings? See JUDGE, GERVAIS, *Intellectual Property: The Law in Canada*, cit., 262.

[55] HAGEN, ENGFIELD, *Canadian Copyright Reform: P2P Sharing, Making Available and the Three-Step Test*, cit., 488.

[56] *Private Copying 2003-2004*, 44.

[57] JUDGE, GERVAIS, *Intellectual Property: The Law in Canada*, cit., 185 and 265.

[58] *Canadian Private Copying Collective v. Canadian Storage Media Alliance*, [2005] 2 F.C.R. 654, paras. 151-157.

If anything, in the Court's view in *BMG* the file sharers' act would have been a "making available" of the copies of the songs. The right to make available is included in the WIPO Copyright Treaty, as well as in the WIPO Performances and Phonograms Treaty, which Canada signed in 1996; but the Treaties have not been implemented yet. In particular, art. 8 of the Copyright Treaty states that "authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the *making available to the public* of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them". A similar right is recognized also for fixed performances and phonographs, by the Performances and Phonogram Treaty[59].

Canada had up to now tried to give execution to both WIPO Treaties with three different Bills, none of which was ever enacted, due to the fall of the Government.

The first of these bills was C-60 "*An Act to Amend Copyright Act*" presented in 2005[60]. The Bill was intended to insert a new paragraph in the *Copyright Act*, 2.4(1)(a), reading as follows: "a person who makes a work or other subject-matter available to the public in a way that allows members of the public to access it through telecommunication from a place and at a time individually chosen by them communicates it to the public by telecommunication"[61]. This provision, creating a new "make available" right, had been saluted by the content industry as the awaited answer to file-sharing[62], due also to the rhetoric which was accompanying the Bill[63].

---

[59] Cf. WPPT art. 10 – *Right of Making Available of Fixed Performances*: "Performers shall enjoy the exclusive right of authorizing the making available to the public of their performances fixed in phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them" and art. 14 – *Right of Making Available of Phonograms*: "Producers of phonograms shall enjoy the exclusive right of authorizing the making available to the public of their phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them".

[60] Bill C-60, *An Act to amend the Copyright Act*, 38th Canadian Parliament, 1st Session, 2005, available at: http://www.parl.gc.ca/content/hoc/Bills/381/Government/C-60/C-60_1/C-60_1.PDF.

[61] Bill C-60, s. 2.

[62] D. FEWER, *Making Available: Existential Inquiries*, 271, in M. GEIST (ed.), *In the Public Interest: the Future of Canadian Copyright Law*, Toronto, 2005.

[63] Cf. for example the *Legislative Summary* of Bill C-60, specifically at pages 1-2, which can be found at the URL: http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/38/1/c60-e.pdf. See the interesting analysis of L. MURRAY, *Copyright Talk: Patterns and Pitfalls in Canadian Policy Discourses*, 15, spec. 27 ff., in M. GEIST (ed.), *In the Public Interest: the Future of Canadian*

The Bill would have not anyway added a new distribution rights; rather, it would have enlarged the already existing communication right[64]. Moreover, for what P2P was concerned, Bill C-60 did not address the liability of the downloader, leaving space for the legality of the downloading[65]. C-60 would have introduced a new series of infringements related to downstream uses of copies made under section 80(1) when a consumer transmitted the copy to the public, or to one or more persons in particular, by telecommunication[66]. The Bill would have also introduced a regulation for technological protection measures and digital rights management[67], as well as a new regime for ISPs' liability. The bill passed the First Reading but could not be approved due to a non-confidence motion which let to a dissolution of the Parliament.

The second bill was C-61 of 2008[68]. As its predecessor, this bill was conceived as a way to implement the WIPO Treaties. Again, this would have included a "make available" right, as well as norms protecting technological protection measures and digital rights management. However, as its antecedent, the bill could not be approved since the Parliament was dissolved and new elections were called.

The third attempt made in 2010 is represented by bill C-32[69], which can be cited as *Copyright Modernization Act*[70]. Exactly as the precedent two bills, this was meant to bring Canada in line with the WIPO Treaties. The Bill had mainly the same content of the previous one, at the same time enlarging the province of fair dealing and other exceptions[71]. For what copyright infringement and ISPs are concerned, the bill would institute a Canadian version of the "notice-and-takedown" procedure existing in the USA. The Canadian "notice-and-notice" system would require ISPs to forward

---

Copyright Law, Toronto, 2005 accessible at: http://www.irwinlaw.com/pages/in-the-public-interest--the-future-of-canadian-copyright-law.

[64] HAGEN, ENGFIELD, *Canadian Copyright Reform: P2P Sharing, Making Available and the Three-Step Test*, cit., 494. FEWER, *Making Available: Existential Inquiries*, cit., 273, who analyzed also the nature of the making available right in general and the aspect it has acquired in each signatory country (spec. 274 f). See also J. GINSBURG, T*he (New?) Right Of Making Available To The Public*, 234 in D. VAVER, L. BENTLY (eds.), *Intellectual Property in the New Millennium, Essays in Honour of William R. Cornish*, Cambridge, 2004, questioning the nature and scope of this right.

[65] FEWER, *Making Available: Existential Inquiries*, cit., 281.

[66] Bill C-60, s. 15.

[67] Bill C-60, s. 27.

[68] Bill C-61, *An Act to amend the Copyright Act*, 39th Canadian Parliament, 2nd Session, 2008, available at: http://www.parl.gc.ca/content/hoc/Bills/392/Government/C-61/C-61_1/C-61_1.PDF.

[69] Bill C-32, *An Act to amend the Copyright Act*, 40th Canadian Parliament, 3rd Session, 2010, available at: http://www.parl.gc.ca/content/hoc/Bills/403/Government/C-32/C-32_1/C-32_1.PDF.

[70] Bill C-32, s. 1.

[71] For a brief explanation of fair dealing, see later in this chapter.

notice of claimed infringement to the user in order to avoid paying statutory damages[72]. This system has been created by Canadian ISPs that have been actually using it for some time now[73]. The bill would also create a new exception, significantly known as "the YouTube exception", that would allow users to create "mash-ups", a typical user generated content[74]. Bill C-32 was not enacted, again because of a governmental failure.

The latest effort is Bill C-11, which may be cited again as *Copyright Modernization Act*[75]. The Bill, that totally mirrors its predecessor C-32[76], was introduced at the end of September 2011 and it is now pending at Parliament Hill.

The intervention of Canadian legislator cannot be postponed much longer. In fact, as commentators had noticed years ago, "[b]y the time Canadian legislators turn their collective attention to the issues of ISP liability and P2P user and provider liability, they may find that the courts have already created a comprehensive regime that adequately reflects Canadian copyright policy and trends in the international arena"[77]. This is in part true, as it will emerge through this chapter.

3.2 The legal framework personal data protection

The Canadian landscape of personal data protection was deeply modified in 2001, with the coming into effect of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[78].

---

[72] Bill C-32, s. 47.

[73] S. BANNERMAN, *Copyright: Characteristics of Canadian Reform*, 39 in M. GEIST (ed.), *From "Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda*, Toronto, 2010, available at: http://www.irwinlaw.com/store/product/666/from--radical-extremism--to--balanced-copyright-.

[74] Bill C-32, s. 22.

[75] Bill C-11, *An Act to amend the Copyright Act*, 41th Canadian Parliament, 1st Session, 2011, available at: http://www.parl.gc.ca/content/hoc/Bills/411/Government/C-11/C-11_1/C-11_1.PDF.

[76] M. GEIST, *Copyright Is Back: Why Canada is Keeping the Flawed Digital Lock Rules*, September 29, 2011 at http://www.michaelgeist.ca/content/view/6033/125/. For the status of the Bill see http://openparliament.ca/bills/41-1/C-11/.

[77] M.K.J. RUSHTON, V.H.L. JONES, *The Tortoise and The Hare: Canadian Legislative Copyright Reforms Race Against Copyright Infringement Over Kazaa And Other New Generation Peer-To-Peer Networks*, 32 AIPLA Q. J. 197 (2004), 242.

[78] From January 1st 2004 the Act is applicable to all commercial activities in each province that has not passed "substantially similar" legislation. See infra note n. 588 For a history of the adoption of PIPEDA, see S. PERRIN, H.H. BLACK, D.H. FLAHERTY, T. MURRAY RANKIN, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, Toronto, 2001, 1 ff.

PIPEDA was based on the Guidelines of the Organisation for Economic Co-operation and Development (OECD)[79]. The OECD was the first international organism that sought to harmonize the protection of personal information. In 1980 the Member States issued some *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines)[80]. Despite these guidelines are voluntary and do not therefore have the force of laws, they provided the basis for most privacy protection schemes adopted by many Member States[81].

The novelty of the PIPEDA was that, for the first time, the collection, the use and the disclosure of personal information was regulated in the *private* sector[82]. Earlier, regulation of personal information in the private sector was a patchwork, and was related only to some sectors of the economy[83]. This first part of PIPEDA was a response to the fears and worries linked to digital technologies, as PIPEDA itself explains: "[t]he purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances"[84].

[79] PERRIN ET AL., *The Personal Information Protection and Electronic Documents Act*, cit., 22; W.A. CHARNETSKI ET AL., *The Personal Information Protection and Electronic Documents Act. A Comprehensive Guide*, Aurora, 2001, 9 according to whom "[t]he eight principles articulated in the OECD Guidelines are analogous to the 10 principles found in the Act" . The OECD is an organization which aim is to promote the social wellbeing of people all over the world, and to improve the economic welfare as well.

[80] The OECD Guidelines related to the handling of personal data can be found at http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html. Canada adhered to the OECD Guidelines in 1984.

[81] The Guidelines include the rights and obligations of individual with regard to the management of personal information and the rights and obligations of organizations with regard to the same matter. These principles can be applied both in the private and in the public sector. The Guidelines comprise some principles intended to be the bases for the regulations later adopted by countries. See B. MCISAAC, R. SHIELDS, K. KLEIN, *The law of privacy in Canada*, Toronto, 2007, 5-2 ff.

[82] See especially Part 1: "Protection of personal information in the private sector". Parts 2 to 5 are instead aimed at "moving federal legislation out of the 'age of paper'", see PERRIN ET AL., *The Personal Information Protection and Electronic Documents Act*, cit., 125 ff. and C.H.H. MCNAIRN, *A Guide to the Personal Information Protection and Electronic Documents Act*, Markham, 2010, 93 ff. for a comment.

[83] MCISAAC ET AL., *The law of privacy in Canada*, cit., 1-51.

[84] Section 3, PIPEDA. Apparently, PIPEDA was also a response to European privacy legislation of 1995 (DIR. 95/46/EC), given that the European Directive, and the consequent laws enacted by the member states, sets a restriction on the transmission of personal information to jurisdictions outside Europe that lack privacy safeguards. In this regard Canada opted for an approach which differs from

Personal data protection was intended as a tool to regulate the use of personal information by commercial organizations and in addition as a way also to protect privacy[85].

PIPEDA gives a definition of what is "personal information", that is "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization"[86]. The key element is the concept of "identifiability": when a specific data, or a compilation of

---

the US one: the latter has not adopted a comprehensive private sector privacy legislation yet. See MCISAAC ET AL., *The law of privacy in Canada*, cit., 4-3.

[85] PIPEDA explicitly incorporates the principles contained in the Canadian Standards Association's *Model Code for the Protection of Personal Information* of 1996 – CAN/CSA-Q830-96 (see Schedule 1 of PIPEDA). For an overview of the principles: MCISAAC ET AL., *The law of privacy in Canada*, cit., 4-31 ff.; PERRIN ET AL., *The Personal Information Protection and Electronic Documents Act*, cit., 15 ff. and CHARNETSKI ET AL., *The Personal Information Protection and Electronic Documents Act. A Comprehensive Guide*, cit., 38 ff..; for an explanation on how and why CSA's principles were used as a base for PIPEDA and the strengths and weaknesses of this approach see PERRIN ET AL., *The Personal Information Protection and Electronic Documents Act*, cit., 3 ff.

[86] Section 2, PIPEDA. The definition differs consistently from the one in the federal Privacy Act (R.S.C., 1985, c. P-21), Section 3: ""personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing, (*a*) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual, (*b*) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (*c*) any identifying number, symbol or other particular assigned to the individual,(*d*) the address, fingerprints or blood type of the individual, (*e*) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations, (*f*) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, (*g*) the views or opinions of another individual about the individual, (*h*) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (*e*), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and (*i*) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but, for the purposes of sections 7, 8 and 26 and section 19 of the *Access to Information Act [R.S.C., 1985, c. A-1]*, does not include (*j*) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including, (i) the fact that the individual is or was an officer or employee of the government institution, (ii) the title, business address and telephone number of the individual, (iii) the classification, salary range and responsibilities of the position held by the individual, (iv) the name of the individual on a document prepared by the individual in the course of employment, and (v) the personal opinions or views of the individual given in the course of employment, (*k*) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services, (*l*) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and (*m*) information about an individual who has been dead for more than twenty years". For a comparison between the two definitions, see MCNAIRN, *A Guide to the Personal Information Protection and Electronic Documents Act*, cit., 30 ff.

data, is attributable to a specific person then it can constitute personal information. At the same time, a data which potentially could identify a person, such as a first name, does not constitute personal information if, in the circumstances of the case, the organization does not hold any other information on the same person[87]. The Federal Court has adopted the following definition: "[i]nformation will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information"[88]. For my purposes, it is worth noting immediately that, following the just-mentioned reasoning, the Assistant Privacy Commissioner held that IP addresses are personal information, since they could be combined with the records of ISPs to identify users[89].

PIPEDA does not distinguish between sensitive and other kinds of data, due to the idea that it is difficult to state a priori which information could be sensitive since different views on what it is sensitive and what it is not are possible.[90] PIPEDA empowers the Privacy Commissioner, an official who was already responsible for the enforcement of the federal *Privacy Act*[91], to receive complaints, conduct investigations and issue reports on her findings[92]. The Commissioner has also a sort of educational role, since the Privacy Commission has to develop programs and disseminate information to enhance public understanding of PIPEDA, to fulfill and publish research on matters related to the protection of personal information, as well as to encourage the adoption by organizations of appropriate practices[93]. Despite the

[87] This is the interpretation of the Privacy Commissioner in *Your Privacy Responsibilities – A Guide for Businesses and Organizations*, at page 2, available at http://www.priv.gc.ca/information/guide_e.pdf.
[88] *Gordon v. Canada*, 2008 FC 258, par. 34.
[89] See PIPEDA Case Summaries n. 25/2001 – *A Broadcaster Accused of Collecting Personal Information via Web Site*, at http://www.priv.gc.ca/cf-dc/2001/cf-dc_011120_e.cfm; n. 2005/315 – *Web-centred company's safeguards and handling of access request and privacy complaint questioned*, at http://www.priv.gc.ca/cf-dc/2005/315_20050809_03_e.cfm; n. 2005/319 – *ISP's anti-spam measures questioned*, available at http://www.priv.gc.ca/cf-dc/2005/319_20051103_e.cfm: "an IP address can be considered personal information if it can be associated with an identifiable individual. […] For the purposes of this complaint, which involved the sending of e-mail by the complainant, the Assistant Commissioner accepted that the originating IP address identified the complainant and was therefore his personal information, as per section 2" of PIPEDA.
[90] PERRIN ET AL., *The Personal Information Protection and Electronic Documents Act*, cit., 23. On this point the Canadian regulation differs sensitively from the European – and Italian – ones. See next chapter.
[91] R.S.C. 1985, c. H-6, see *infra*. MCISAAC ET AL., *The law of privacy in Canada*, cit., 3-22 ff.
[92] Sections 11-12 and 18-19, PIPEDA.
[93] Section 24, PIPEDA.

tasks assigned, the Commissioner does not have the power to issue rulings or make orders, which is reserved to the Federal Court of Canada[94].

PIPEDA applies to all organizations in respect of personal information that the organization collects, uses or discloses in commercial activities. It applies also to information, related to employees of an organization, that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business. It is not applicable to any federal governmental institution to which the *Privacy Act* applies; nor to individuals that collect, use or disclose personal information only and solely for personal or domestic purposes; nor to organizations which collect, use or disclose these personal data for journalistic, artistic or literary purposes and not for any other purposes[95].

One of the most important and maybe most controversial principles of PIPEDA is "consent"[96]. Consent given by the person concerned is required whenever her personal information is dealt with by somebody else, except where inappropriate[97]. Consent should be "informed", that is, the organization shall make a reasonable effort to ensure that the person is advised of the purposes for which her data are used. The purposes must be formulated in a manner that the person can reasonably understand them. Consent may be given in many different ways and may be withdraw at any time[98]. Nevertheless there are some circumstances in which PIPEDA replaces express consent with situations in which consent is sort of "assumed"[99]. The Privacy Commissioner has pointed out that the mere fact that a collection of personal data is "reasonable" does not erase by itself the need for consent[100]. Specifically, Section 7(3)(c) permits the disclosure of personal information in response to "a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to

[94] MCISAAC ET AL., *The law of privacy in Canada*, cit., 4-21.
[95] Sections 4(1) and 4(2), PIPEDA.
[96] For a critical approach to the centrality of consent in PIPEDA: L.M. AUSTIN, *Is Consent the Foundation of Fair Information Practices? Canada's Experience under Pipeda*, 56 University of Toronto Law Journal 181 (2006).
[97] PIPEDA, Schedule 1 – "Principles Set Out In The National Standard Of Canada Entitled *Model Code For The Protection Of Personal Information*, CAN/CSA-Q830-96" – 4.3 Principle 3 Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.
[98] PERRIN ET AL., *The Personal Information Protection and Electronic Documents Act*, cit., 22 ff.
[99] Sections 7(1)-(3), PIPEDA.
[100] MCISAAC ET AL., *The law of privacy in Canada*, cit., 4-45.

comply with rules of court relating to the production of records". This provision will be particularly significant in the following part of this work.

At the time PIPEDA was enacted, only Québec had already enacted its own legislation regarding personal information for the private sector, and this in existence since 1994[101]. It was later, in 2004, that British Columbia and Alberta promulgated their statutes[102]. All these regulations are substantially similar to PIPEDA; therefore the collection, use and disclosure of personal information in these provinces will be governed by these laws. In the case that personal information is sent out of the province, the federal legislation will apply[103].

As far as the protection of personal information in the public sector is concerned, federal and provincial laws were enacted well before PIPEDA. At the federal level, the first regulation came into place in 1977 with the enactment of the *Canadian Human Rights Act*[104]. In 1983, the provision dealing with the protection of personal information was repealed from the *Canadian Human Rights Act* and the matter has been regulated by the already mentioned federal *Privacy Act* ever since. The *Privacy Act* concerns both the collection and use of personal information by federal government department and agencies, and the right of access for individuals to their data. The Privacy Act introduced a Privacy Commissioner, who has the power to make recommendations for the collection and use of personal information and for the correctness of decisions denying access to personal information.

[101] *Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1. Québec had also included a constitutional protection for privacy: Section 5 of the *Québec Charter of Human Rights and Freedoms* states that "[e]very person has a right to respect for his private life", see R.S.Q., c. C-12, s. 5. Furthermore, the *Civil Code of Québec*, as amended in 1987, provides in its Chapter III norms for the "Respect of Reputation and Privacy" (S.Q., 1991, c. 64, arts. 35-41).

[102] British Columbia *Personal Information Protection Act*, S.B.C. 2003, c. 63 and Alberta *Personal Information Protection Act,* S.A. 2003, c. P-6.5. These Acts, as well as the Québec one, apply to a wider compass than the federal Act: see MCISAAC ET AL., *The law of privacy in Canada*, cit., 4-56 ff., also with regard to problems concerning the relation between provincial and federal Personal Information Acts. Despite Ontario announced that would have implemented its own legislation, up to now this has not happened yet. The Province has nevertheless introduced a Personal Health Information Privacy Act in 2000, which provides rules for the management of personal health information: *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Schedule A [*PHIPA*].

[103] MCISAAC ET AL., *The law of privacy in Canada*, cit., 4-55.

[104] S.C. 1976-77, c. 33, R.S.C. 1985, c. H-6. Section 2(b) provided: "the privacy of individuals and their right of access to records containing personal information concerning them by any purpose including the purpose of ensuring accuracy and completeness should be protected to the greatest extent consistent with the public interest".

However, the Commissioner does not have the power to make binding orders, which are reserved to the Federal Court[105].

This Act applies to government institutions, i.e. to all government departments, bodies and offices. As already said, the definition of "personal information" given in the Privacy Act is different from the one contained in PIPEDA, since the former is much more detailed than the latter[106]. As opposed to what happened for the protection of personal information in the private sector, regulations of access to information and privacy have been enacted by most provinces and territories of Canada, except New Brunswick[107].

As explained above, PIPEDA has been conceived as a way to improve privacy protection by adding protection for personal information in the private sector. Indeed, the collection and use of personal information, both in the private and in the public sector, can have a great impact on an individual's privacy. It is probably due to this fact that the two concepts are often overlapping. As already mentioned earlier in this work, I borrow this overlap in conducting my analysis, just as lawmakers have done.

Apart from statutory provisions, privacy is contemplated, even if not directly, by the Canadian *Charter or Rights and Freedoms*[108]. More precisely, Section 7 of the

[105] MCISAAC ET AL., *The law of privacy in Canada*, cit., 3-5. It has been asserted that the *Privacy Act* should be reformed, given that it is more than twenty five years old. Furthermore, due to the enactment of PIPEDA government departments and agencies are nowadays subject to a lower standard for the management of personal data; see D.H. FLAHERTY, *Reflection on Reform of Federal* Privacy Act, Publications of the Office of the Privacy Commissioner of Canada, 2008, available at http://www.priv.gc.ca/information/pub/pa_ref_df_e.cfm.

[106] See *supra* note n. 571.

[107] See: *Freedom of Information and protection of Privacy Act*, R.S.B.C. 1996, c. 165 (B.C.); *Freedom of Information and protection of Privacy Act*, S.A. 1994, c.. F-18.5 (Alberta); *Freedom of Information and protection of Privacy Act*, S.S. 1990-91, c. F-22.01 (Sask.); *Local Authority Freedom of Information and protection of Privacy Act*, S.M. 1997 c. 50 (Man.); *Freedom of Information and protection of Privacy Act*, R.S.O. 1990, F.31, c. M. 56 (ON); *Municipal Freedom of Information and protection of Privacy Act*, R.S.O. 1990, c. M. 56 (ON); *An Act respecting Access to document held by public bodies and the Protection of Personal Information*, R.S.Q., c. A-2.1 (Qc); *Freedom of Information and protection of Privacy Act*, S.N.S. 1993, c. 5 (N.S.); *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A-1.1; *Access to Information and Protection of Privacy Act*, S.Y.T. 1995, c. 1 (Yukon); *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20 (N.W.T.). For an overview: MCISAAC ET AL., *The law of privacy in Canada*, cit., 3-34 ff.

[108] In 1987, the Canadian House of Commons' Justice Committee suggested that serious consideration should have posed to the idea of creating a constitutional right to privacy. The idea, clearly, did not pass. The Committee's outcome is cited by D.H. FLAHERTY, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 Case W. Res. L. Rev. 831 (1991), 843. The Author discusses the feasibility and utility of introducing a right to privacy in the Canadian Constitution and expresses some doubts on it. See especially 849 ff.

Charter states that "[e]veryone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice"[109]. There is growing consensus, also in the Supreme Court's jurisprudence[110], that section 7 may be a source of constitutional protection for privacy. In the case *R. v. O'Connor*, for example, an accused of sexual assault wanted to have access to the complainant's medical records. It was a case of "third party discovery"[111], and the Court had to weigh the interest of the complainant in the records against the right of the accused to obtain full information. The first step was to understand whether the complainant had a privacy interest in those records or not. All the judges agreed on the fact that the Charter gives constitutional protection to the right to privacy, but the most clear and firm judgment was that of L'Heureux-Dubé J. She held that therapeutic records implied a reasonable expectation of privacy, which is worthy of the protection of Section 7[112]. Later on, other decisions expressly supported this view[113]. In the more recent case of *R. v.* Mills, however, judges concluded that privacy had to be traced back to Section 8[114], rather than 7[115]. Despite the fact that the issue was very close to the one decided in *R. v. O'Connor* (the production of complainants' private records in sexual assault proceedings), the Court in *Mills* held that an order to produce records would be a search or seizure matter and, therefore, comprised in Section 8[116]. This different approach has been explained as follows: "courts will protect the privacy right under the rubric of section 8 wherever a search or seizure occurs. However, if there is no search or seizure made by the government, then section 7 may serve as the source of constitutional protection of the right to privacy"[117]. Hence, privacy finds two different roots in the

[109] Section 7, Charter of Rights and Freedoms, "Life, liberty and security of person".
[110] See for example *R. v. O'Connor*, [1995] 4 S.C.R. 411.
[111] For an explanation of what discovery and third party discovery are, see later in this chapter.
[112] *R. v. O'Connor*, cit., par. 119.
[113] For example in a case close to the mentioned *R. v. O'Connor*, *M. (A.) v. Ryan*, [1997] 1. S.C.R. 157, par. 80, the Court stated: "the rights to individual liberty and security of the person as enshrined in s. 7 of the Charter encompassed a right to privacy. This finding was based on a number of developments in the jurisprudence of this Court. In its s. 7 jurisprudence, it has expressed great sympathy with the notion that liberty and security of the person involve privacy interests".
[114] Section 8, Charter of Rights and Freedoms, "Search or seizure": "Everyone has the right to be secure against unreasonable search or seizure".
[115] *R. v. Mills*, [1999] 3 S.C.R. 668.
[116] *R. v. Mills*, cit., par. 62.
[117] MCISAAC ET AL., *The law of privacy in Canada*, cit., 2-9.

Charter of Rights and Freedoms, which can alternatively be invoked depending on the type of intrusion privacy suffers.

Three different "zones" of privacy have been recognized in the case law:

1. territorial, such as the one a person should enjoy in her home;
2. personal or corporeal, related to human body and physical personality;
3. informational, protecting intimate details of people[118]. Indeed, the ability to control the dissemination of personal information is part of the right to privacy[119].

Furthermore, there are two barometers to be applied in understanding the extent of a person's right to privacy, which are: a) the degree to which an individual's liberty or security is threatened by the state's intrusion into a person's private affairs, and b) the extent of the individual's reasonable expectation of privacy[120]. This latter issue is protected primarily by the already mentioned Section 8. In the case law, this section has been interpreted as protecting people and not places[121]. It is important to remember that the Charter only applies to Crown actions – governments and other state actors -- and therefore, even if it has an important role, it would hardly be useful in protecting citizens in their exchange of personal information in the private sector[122].

According to the case law, to concretely address the existence and depth of a reasonable expectation of privacy, courts should consider a case-by-case analysis[123]. The need for privacy can indeed be different accordingly to the circumstances; therefore, the investigation on whether a reasonable expectation of privacy exists has

[118] *Ruby v. Canada (Attorney General)*, [2000] 3 F.C. 589 (C.A.), par. 166. But see already *R. v. Dyment*, [1988] 2 S.C.R. 417, par. 30, citing *Privacy and Computers* (Ottawa, 1972), a report of the Task force established by the Department of Communications and the Department of Justice of Canada.
[119] *Ruby v. Canada (Attorney General)*, cit., par. 169.
[120] *Ruby v. Canada (Attorney General)*, cit., par. 168.
[121] *Hunter v. Southam Inc*., [1984] 2 S.C.R. 145, par. 23, where the Supreme Court of Canada made reference to the US Supreme Court seminal case *Katz v. United States*, cit. *Hunter v. Southam Inc*. was a decision in the criminal context, therefore the requirements and thresholds applied there can differ from those used in a civil lawsuit: see MCISAAC ET AL., *The law of privacy in Canada*, cit., 2-17.
[122] PERRIN ET AL., *The Personal Information Protection and Electronic Documents Act*, cit., 7.
[123] In *R. v. Edwards*, [1996] 1 S.C.R 128, par. 45, the Supreme Court listed a number of factors which should be taken into consideration in order to assess the expectation of privacy.

to be "factually" driven[124]. This means taking into account objective and subjective elements[125]. Courts must understand the privacy component of a specific right or freedom. Once determined that a privacy element exists, then judges can value whether the limits imposed on privacy are reasonable or not[126].

The concept of a "reasonable expectation of privacy" has been applied also to computer surveillance and other technology-related cases. Just to give an example, the Alberta Court of Appeal had to decide on a case that involved a privacy issue related to an e-mail account maintained by an ISP[127]. A man was accused of possessing child pornography. The ISP, in a routine repair of the man's e-mail box, discovered an e-mail attachment containing child pornography and therefore informed the police and copied the e-mail and attachment to the police. In the process, the man's defence claimed a breach of his privacy to his e-mails and a breach of his Charter rights. His defence held that the man had a reasonable expectation of privacy over his e-mails, exactly in the same way he would have on his "first class" mail. The Court concluded that, indeed, e-mails carry a reasonable expectation of privacy, but, given the way in which this technology was managed, the degree of privacy was less than the one offered to first class mail. Therefore, the search the ISP and the police made on the accused's personal computer was lawful and legitimate[128].

As one can understand from this brief overview, the concept of privacy has been given a great deal of recent attention in Canada. It is a right which has been traced back to the Charter of Rights and Freedom by both scholars and courts. And this has happened even if the Charter never explicitly mentions physical privacy, let alone information privacy. Nevertheless, courts have given such an important place to this right that there is no pre-determined solution for privacy cases. A case-by-case analysis with a balancing test is usually applied[129], stressing the above-mentioned

[124] See for example *R. v. Colarusso*, [1994] 1 S.C.R. 20, par. 19 and *R. v. Wong*, [1990] 3 S.C.R. 36, par. 47.
[125] For an example of questions to be asked in order to understand whether there is a reasonable expectation of privacy, see *R. v. Tessling*, [2004] 3 S.C.R. 432, paras. 32 ff.
[126] FLAHERTY, *On the Utility of Constitutional Rights to Privacy and Data Protection*, cit., 845.
[127] *R. v. Weir* (1998), 59 Alta. L.R. (3d) 319 (Q.B.).
[128] *R. v. Weir* (1998), cit., paras. 56-77 *sic passim*.
[129] See also later in this chapter for other examples of balancing tests applied.

magnitude of this right. The uncertainty related to this right could be one of the reasons why judicial opinions sometime differ greatly among each other.

The next sections will show how copyright and privacy are treated in the Canadian context when one collides with the other.

3.3 Cases and possible solutions

3.3.1 BMG

It is said that, in the age of globalization, boundaries are disappearing. What happens in another country, or even in another continent, affects the events of other countries or continents. Law and its application are not an exception. Therefore, as it is often the case, some time after the first cases in the USA, Canadian copyright holders started their own war against file sharing on Canadian "soil"[130].

In February 2004 BMG Canada[131], together with other companies holding copyright in sound recordings filed a claim against "John Doe, Jane Doe and All Those Persons Who Are Infringing The Plaintiffs' Copyright in Sound Recordings". The plaintiffs were the largest record companies in Canada, and are collectively hereinafter called CRIA, after the umbrella group Canadian Recording Industry Association that represented them on the pleadings[132]. CRIA's suit was a sort of copycat version of the RIAA's ones, given they had the same goals referring to public education and deterrence, and that CRIA was the RIAA arm in Canada.[133]

The respondents were five ISPs, namely Shaw Communication Inc., Rogers Cable Communication Inc., Bell Sympatico, Telus Inc. and Vidéotron Ltée. CRIA's

[130] Prof. Michael Geist reports that Canadian courts first faced the issue of online anonymity in 1998. The case, decided in Ontario, revolved around an allegedly fraudulent posting made to a stock chat room. Through a John Doe suit, the ISP was ordered to release its users' names and many other information regarding them. See M. GEIST, *Internet Law in Canada*, Concord, 2002, 377 ff.

[131] "BMG is an international group of music companies focused on the management of music rights", see http://www.bmg.com/category/about-us.

[132] The Canadian Recording Industry Association is a non-profit organization, founded in the sixties, to represent the interest of Canadian companies that create, manufacture and market sound recording. The association also enforces the rights of its members; see http://www.cria.ca/about.php and http://www.cria.ca/whatwedo.php.

[133] J. BAILEY, *The Substance of Procedure: Non-Party Disclosure in the Canadian and U.S. Online Music Sharing Litigation*, 43 Alta L. Rev. 615, 625 (2006). For the educational campaign carried on by CRIA, see http://www.cria.ca/news/130204a_n.php. Since basically this is the only case faced by Canadian court with respect to the problem of balancing copyright enforcement and privacy concerns, my analysis will be it much deeper than the one made for the American cases in the previous chapter.

first move was to issue a statement of claim against 29 "Does" idenetified by IP addresses and move for discovery from the involved ISPs in order to ascertain their real identities. Basically, CRIA had to start directly from what for the RIAA was only the second step, since in Canada there is no instrument such as the section 512(h) of DMCA. Plaintiffs relied on Rules 233 and 238 of the Federal Court Rules to compel the providers to disclose individuals' information[134].

These rules look at the disclosure of documents from non-parties as a component of discovery. "Discovery of documents" or "productions" gives each party the possibility to access documents that may be relevant to their claim or defense, which are in possession of other party – or, as in this case, of a non-party. Documentary discovery involves two steps: disclosure and production. Examination for discovery, then, enables parties to ask questions of representatives of the other party[135].

According to Rule 233(1), examination can be ordered "if the document is relevant and its production could be compelled at trial". Usually in Canada discovery is limited to parties to the proceeding. Nevertheless, in exceptional cases and in the instance of a motion such as CRIA's, the court can order production of documents in the possession, control or power of a person who is not a party. This happens only when it would be unfair to require the moving party to proceed to trial without obtaining the discovery of the document. In order to evaluate the fairness of such an action, different criteria have been considered: normally, however, the threshold or perceived unfairness is high, so as to limit the cases where such disclosure will be compelled[136].

Rule 238 refers to the examination of non-parties. Also in this case there is the belief that only in exceptional circumstances a non-party can be asked to supply information for a case. Yet there are times in which information critical to the preparation of a party's case are available only for a non-party. As a result, there are rules that provide for tests aimed at granting the possibility of examining a non-party. These tests generally require the requesting party to show the existence of certain conditions. In order to decide whether the leave to examine should be granted, courts

[134] *Federal Court Rules*, 1998, S.O.R./98-106 [FCR].
[135] WALKER, SOSSIN, *Civil Litigation*, cit., 167-170.
[136] WALKER, SOSSIN, *Civil Litigation*, cit., 179.

normally balance the interest of the party seeking the examination with the interest of the party being sought to be examined[137]. Rule 238(3) determines when a court may grant leave: "if it is satisfied that (a) the person may have information on an issue in the action; (b) the party has been unable to obtain the information informally from the person or from another source by any other reasonable means; (c) it would be unfair not to allow the party an opportunity to question the person before trial; and (d) the questioning will not cause undue delay, inconvenience or expense to the person or to the other parties". As we shall see, the interpretation of these rules was crucial in more than one case regarding intellectual property rights enforcement.

Going back to the facts of the *BMG* trial, CRIA's notice of motion stated that an investigation conducted for them revealed that file-sharers had infringed plaintiffs' copyright. In particular CRIA relied on MediaSentry, a company providing service for locating and identifying IP addresses engaged in file-sharing activities. To do so, the company used a particular software, called "MediaDecoy". This was a program that distributed bogus or inoperative files over the Internet. Users would download them thinking they were music files. These files were made to look like real music files, but they instead were inoperative[138].

As was the case in the RIAA's cases, these people were identifiable only through pseudonyms and their IP addresses. These IP addresses were registered with one of the respondent ISPs. CRIA claimed that without disclosure of the users' identities, its members could not enforce their rights. Therefore, it asked for obtaining "the last known name; home, mailing and business addresses; telephone numbers; facsimile numbers and e-mail addresses in the business records of the ISP associated with the IP Addresses and dates and times listed in [an attached schedule]" as well as "a copy of the ISP's records used to identify the information

[137] WALKER, SOSSIN, *Civil Litigation*, cit., 186.

[138] See Shaw's Written representations available at http://www.cippic.ca/documents/file-sharing-lawsuits/FurtherWrittenSubmissionsShaw.pdf, at 14 [*Shaw's Written representations*]. Documents of the trial are available on the website of the Canadian Internet Policy and Public Interest Clinic – CIPPIC, which intervened in the process as a public interest group (www.cippic.ca), see CRIA's request order for ISPs available at http://www.cippic.ca/documents/file-sharing-lawsuits/Schedule-A--Order.pdf.

disclosed pursuant to subparagraph (a), which copies may be redacted by the ISP prior to production to remove irrelevant information"[139].

Four out of five ISPs opposed to the motion, Vidéotron the only accommodating one[140].

The analysis will now describe the argument advanced by every actor in the trial, in order to better understand their positions and the interests at stake.

a) Shaw's response

The ISP Shaw explained first of all how IP addresses (or IP numbers) are assigned to its customers. These numbers are dynamic, meaning that the addresses assigned are changeable, and not fixed, as static IP addresses would be. When a device attaches through Shaw's system to the Internet, the ISP assigns an IP address automatically. When the device disconnects from the system, the same IP address may be re-assigned to another device. The use of this system allows more devices to be connected easily through the ISP system. For this reason, this methodology is by far the most common through present ISPs.

Despite this continual re-assignment of IP addresses, Shaw does maintain logs of when a given IP address is assigned to a particular Media Access Control (MAC, such as a particular electronic device). However, the system stores neither cable modem serial number, nor the customer account. Therefore Shaw could not tell which IP address was assigned to a subscriber in the past. Even if Shaw was able to identify an account and its subscriber, obviously it could not identify the actual person using the device at that time. In no way could Shaw determine which subscriber account was assigned to the IP addresses referred by the plaintiff with the degree of certainty required in a sworn statement[141].

Shaw then pointed out that revealing subscribers' information could make it liable under PIPEDA, especially in case of incorrect information. The ISP illustrated its terms of use, where the company acknowledges that "[c]ustomer privacy is a high priority at Shaw as we have always maintained a policy of protecting our customers'

[139] Paras. 1(a) and (b) of the order in *BMG I*, available at http://www.cippic.ca/sites/default/files/file-sharing-lawsuits/Schedule-A--Order.pdf.
[140] For the complete documents see ISPs' written representations, available at http://www.cippic.ca/documents/file-sharing-lawsuits/document-archives.html.
[141] *Shaw's Written representations*, 10-11.

personal information". By its own admission, Shaw's response to CRIA's claim was largely based on the commitment the company took with its customers, which, in turn, was applied to effectively implement the principles contained in PIPEDA[142]. Shaw then underlined the importance of privacy in the Canadian system, quoting a Supreme Court case sentence: "privacy is essential for the well-being of the individual"[143].

According to Shaw's written representations, its customers have a reasonable expectation that information about them will remain confidential. While PIPEDA provides some basis for disclosure of personal information, "it should be noted that there is no provision in PIPEDA for making such an order on an *ex parte* basis *vis-à-vis* the person whose personal information is sought"[144]. Given these doubts, the ISP suggests asking three questions: "(a) must the inquiry process that the Plaintiffs seek to invoke be used in the case in which the order is made? (b) can it be used in another case not yet started? (c) can it be used to start "settlement" negotiations with an identified person?". In Shaw's opinion permitting a party to have access to individuals' personal information for engaging an individual in settlement discussions (like CRIA was probably trying to do), would be antithetical to the purposes and principles of PIPEDA.

Shaw's representation also examined the application and interpretation of discovery rules related to the case. With regard to Rule 233, Shaw acknowledges that the rule is limited in scope. This rule permits an order for production of any document in possession of a non-party if "its production could be compelled at trial". According to the ISP's view, the expression "at trial" would imply that the document would be used in the case in which party's motion is brought and not in a possible future action or proceeding. Shaw drew the same conclusions for the application of Rule 238, regarding third-party discovery, given that Rule 238(1) could only be used in specific circumstances and requirements. In particular, as above mentioned, a court may order third party a discovery where, among other requirements, it would be unfair not to allow the party an opportunity to question the person before trial and the questioning will not cause inconvenience or expenses to the other parties. In Shaw's view, the permission of

[142] *Shaw's Written representations*, 6.
[143] *R. v. Dyment*, cit., par. 28.
[144] *Shaw's Written representations*, 17.

discovery would give CRIA the opportunity of a "fishing expedition", which is not allowed under Canadian case law. In the respondent's view the plaintiffs were seeking more a civil search warrant rather than a discovery. Indeed, the information asked by CRIA would have not been used in the case against the ISPs, but to actually start a new case. Given the US scenario of RIAA's cases, Shaw believed that CRIA, once obtained users' information, would have tried to settle with them[145].

Shaw then relied on the submissions made by Canadian Internet Policy and Public Interest Clinic (CIPPIC), intervening as a public interest group[146]. These submissions stated that the court should have applied a higher threshold, such as a strong *prima facie* case, prior to ordering disclosure, since there was another competing interest at stake: privacy. On the top of that, in this case the targets, i.e. users, were not even before the court.

The ISP argued that CRIA was far from showing a strong *prima facie* case of copyright infringement against the Does. The plaintiffs declared they own the copyright on various recordings listed in the Statement of Claim, but, according to Shaw, they had not presented direct evidence of copyright infringement. Indeed, the affidavits on which plaintiffs based their assertions seemed to be quite unreliable[147]. To give an example, Shaw reported that Mr. Millin, who was the president of MediaSentry, had not listened to any of the files downloaded by that company in order to confirm that the files downloaded corresponded to those in which plaintiffs claimed copyright or if they were just bogus files[148].

[145] *Shaw's Written representations*, 18 ff. *sic passim.*

[146] "The Canadian Internet Policy and Public Interest Clinic (CIPPIC) was established at the University of Ottawa, Faculty of Law in the fall of 2003. It is the first legal clinic of its kind in Canada". CIPPIC declares to have a twofold mission: to fill voids in public policy debates on technology law issues, providing under-represented individuals and organization with legal assistance and to provide a high qualify and rewarding legal education experience to students of law attending the clinic. See http://www.cippic.ca/en/about-us.

[147] An affidavit is an "evidentiary instrument of one witness, made in writing and attested to by the path or affirmation of the witness". The word "affidavit" come from Latin and means "he had declared upon oath". Affidavits differ from depositions. The former are statement of evidence made *ex parte*, without cross-examination (which can anyway follow). Depositions are declarations of facts given under oath, such an affidavit. However, deposition are given by witnesses who are subject to cross-examination; only after that, evidence is reduced to writing. Cf. ABRAMS, MCGUINNES, *Canadian Civil Procedure Law*, cit., 840 ff.

[148] The same could be said for Ms. Yonekura, the Anti-Piracy Coordinator for CRIA.

For all the reported reasons, Shaw asked the court not to allow the privacy rights of John and Jane Doe defendants to be violated on the basis of the weak records presented by the plaintiffs[149].

b) Rogers' response

In its written representations[150], Rogers immediately clarified that for eight out of the nine requested IP addresses, it could identify only one last known name and address within six days of the date sought in CRIA's motion. Rogers did not have information regarding the exact date and time requested by the plaintiffs. Unlike Shaw, Rogers had notified the eight identified account holders, despite the notice reached only seven of the eight people[151].

Roger then addressed the issue of privacy and underlined that a potential order for the disclosure of personal information would need to comply with PIPEDA principles. In this respect the ISP cited the landmark case *Glaxo Wellcome*[152], on which the Court will later greatly rely. Further, the respondent pointed out that, in case of an order for disclosure, this should be limited to last known name and address, since asking for business addresses, telephone numbers, facsimile numbers, and email addresses would be "overbroad, excessive and should not be required". Since this information would have gone beyond what was necessary for the plaintiffs, its disclosure would have been in contrast with PIPEDA, which requires that only reasonably necessary personal information be disclosed[153].

c) Bell Sympatico's response

Bell's response started with privacy concerns[154], acknowledging that those requested by the plaintiffs could surely be considered personal data under the PIPEDA. Bell argued that the enactment of the mentioned Act entitled the citizens to a high expectation of privacy in their personal information. In accordance with this

[149] Finally Shaw took into account the problem of the expenses the company would have borne to collect and verify the documentation requested by CRIA. *Shaw's Written representations*, 20 ff.

[150] Available at http://www.cippic.ca/documents/file-sharing-lawsuits/Rogers_Written_Reps_Mar12.pdf [*Rogers' written representations*].

[151] After explaining this, the ISP explicitly stated that the company incurred in at least 3,000 $ expenses for the research of the information requested, see *Rogers' written representations*, 4.

[152] *Glaxo Wellcome PLC v. Minister of National Revenue*, [1998] 4 F.C. 439, par. 20 [*Glaxo Wellcome*]. For an overview of the case see later in this chapter.

[153] *Rogers' written representations*, 6.

[154] Bell's response is available at http://www.cippic.ca/documents/file-sharing-lawsuits/Bell_Written_Submissions.pdf [*Bell's written representations*].

expectation, the PIPEDA allows the disclosure without knowledge or consent of the individual only in very limited cases, as explained earlier in this chapter. Bell said to be willing to disclose this information under an order of the court, but it held that the court should have ordered the disclosure only if CRIA had showed a *prima facie* case. According to Bell's response, a *prima facie* case would exist if "a) the applicants either own(ed) or possess(ed) the exclusive license of relevant copyrights; b) Bell's customers […] identified by the pseudonyms John and Jane Doe ha(d) made available for distribution those copyrights, for the purpose of allowing others to infringe them; and c) such conduct (was) actionable"[155].

Bell's argument was that the affidavits submitted by the plaintiffs were not enough. As required by discovery law, CRIA had submitted three different affidavits, already mentioned: two of Gary Millen and one of Kathy Yonekura. None of these affidavits was based upon personal knowledge, nor on material submitted to the court. Bell underlined that "Rule 81(1) states that affidavits shall be confined to facts within the personal knowledge of the deponent, except on motions in which statements as to the deponent's belief, with the grounds therefor, may be included". When Yonekura said to believe that the defendants were owners of the copyright claimed to be infringed, she said to believe it upon the representations of the applicants. Therefore she did not really know if that was true. Likewise, the affidavits sworn by Millen with regard to the infringement were based on belief and he confirmed, on cross-examination, that he lacked personal knowledge of the investigation related to Bell's customers. Disclosing in this case would mean that the Court would have to base its decision on hearsay. A court can base its decision to allow evidence on hearsay when there is the *necessity* of using such a type of evidence. In this case the court would have determined if the exhibits were admissible only relying on the affidavits and, therefore, *only* on hearsay[156].

Bell then admitted to be able to identify the (only!) customer linked to the IP address given by CRIA. Nevertheless Bell questioned the possibility that a non-party could produce document by serving an affidavit with attached exhibits. Citing *Loblaw Companies Ltd. v. Aliant Telecom, Inc.*[157], the ISP was doubtful whether the

[155] *Bell's written representations*, 2-3.
[156] *Bell's written representations*, 3-4. Emphasis added.
[157] *Loblaw Companies Ltd. v. Aliant Telecom, Inc*., [2003] N.B.R. (2d) (Supp.) No. 32 [*Loblaw*].

request of the applicant could be satisfied. If so, Bell was completely willing to disclose the required information, as long as it was compensated for the expenses, including legal fees[158].

d) Telus's response

Telus was requested to give information on three pseudonymous using KaZaA. The ISP immediately explained that it did not maintain record of Internet usage for the purpose of identifying the account holders or the material accessed or transmitted[159].

The company explained the procedure it should have followed in order to reach for the information asked by the plaintiffs. Telus explained also that even if a person could be identified, this was just the subscriber, who might not be for sure the same person as the alleged infringer. Furthermore, the response stated that, assuming that the information still existed and was recoverable, "[t]he more historic a search is, the less reliable the information [would] be, as record were kept in different ways for different period for different systems". According to Telus, if the request was made within thirty days from the date in which the Internet was accessed to perpetrate the alleged infringing activity, the company had good chances to identify the account holder. For requests concerning activities made thirty days or before, the information would become less and less reliable up to the point of becoming inexistent[160].

Then the respondent addressed again the problem of identifying the "real" alleged infringer. Telus recognized that there was more than one obstacle. Indeed, not only the person acting behind the monitor could be different from the account holder, but there could have been other incongruities. For example, certain institutions or corporations have multiple LANs[161], each with multiple users; a computer may be hacked and be used by the hacker, without the account holder's knowledge; finally, a wireless network might not be secured against external

[158] *Bell's written representations*, 5 ff.

[159] Telus's written representations can as well be found at http://www.cippic.ca/documents/file-sharing-lawsuits/Written_Representations.pdf [*Telus's written representations*]. As the other respondents did, Telus firstly mentioned the issue of expenses and costs borne.

[160] *Telus's written representations*, 4-6, *sic passim*.

[161] A Local Area Network (LAN) is a system in which several computers are linked together by a cable, usually an Ethernet one, so that they form a network. Usually these computers share the use of particular facilities or data, that sometimes are stored in a bigger computer (called server) to which all the other smaller computers are linked. Typically this kind of network is provided inside universities, companies or law firms; see *Entry: LAN*, B.B. SOOKMAN, *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions*, Toronto, 2005, 234.

access[162]. For all the mentioned reasons, Telus could identify only one of the three IP addresses associated with it.

The ISP complained that in case of compliance of the order, the company would incur a great deal of expenses, without considering Telus's own business and customers' needs. Taking also into account the words of one affidavit, Telus was indeed afraid that this could have been just the first of an indefinite number of lawsuits, following the example of the US Recording Industry[163].

Then Telus examined the question under a procedural point of view. Rule 233 permits courts to order the production of a document in possession of a non-party. CRIA had asked for the production of information that was not already available to the ISPs. CRIA's own motion acknowledges this when stating that respondents could have "easily found" the names and addresses. Telus therefore considered plaintiffs' request to be a request for an investigation rather than for the production of already existing documents. This would have meant that the order sought was not within the boundaries of Rule 233[164].

The respondent then referred to the possibility that CRIA could be granted leave to amend its motion to rely upon a decision of the House of Lords, *Norwich*[165], earlier followed by the above cited *Glaxo Wellcome* case In both these cases, non-parties were requested to produce documents, which already existed as a result of their normal functions. The records sought were therefore easily available and their production was questioned under principles other than their very existence. In the actual case Telus would have been forced to invest efforts and money into the searching activity. These expenses made Telus fearful of the scenario in which CRIA were to follow the path taken by RIAA and started a massive number of suits[166]. As a consequence, like all the other respondents already had, the company asked to be indemnified for the efforts it would undertake[167].

The ISP then stressed that the application of the *Norwich* principle would have required a *prima facie* case and a strong intent of the plaintiff to commence the

[162] *Telus's written representations*, 7.
[163] *Telus's written representations*, 8-9.
[164] *Telus's written representations*, 11.
[165] *Norwich Pharmacal Co. v. Commissioners of Customs and Exercise,* [1974] A.C. 133(HL) [*Norwich*].
[166] *Telus's written representations*, 12.
[167] *Telus's written representations*, 14.

proceeding[168]. In fact, a so called "Norwich Order" is an equitable relief that requires an innocent person, who has become involved in the wrongful activity of a third party against the moving party, to provide information necessary for the moving party to pursue a claim against the tortfeasor. The innocent person is subject to an equitable duty to help the victim of the third person's wrongdoing[169]. Telus argued that this kind of relief should not be used just to a "mere gratification of curiosity" or "for some ancillary but lesser purpose than pursuing legitimate action"[170]. In the same way as argued by Bell, Telus wrote that the plaintiffs had not put convincing prove of the infringement; instead, they had relied only on hearsay affidavits. Another requirement of *Norwich* is that the non-party is the *only* source of information, but CRIA did not show its effort in searching for the names using other means. Telus noticed that CRIA did not ask KaZaA directly for the information, even if it probably would have had more direct information[171]. The respondent then clarified that the FC should have balanced the interests of CRIA against the conscripted ISPs[172].

Finally, Telus admitted its fear for the case in which the information given to CRIA would have been wrong. Revealing the name of a wrong person and exposing the same to a lawsuit could be highly costly for the company itself[173].

e) CIPPIC's memorandum of argument

CIPPIC's memorandum of argument from the very beginning stated that the "case involve(d) the balancing of privacy rights of individuals against the need for

[168] Despite the strong prima facie case requirement was necessary according to the Norwich decision, now it seems that in UK this requirement is no longer requested, see C. HOLLANDER, *Norwich Pharmacal takes wings*, 28 Civil Justice Quarterly 458, 460 (2009). According to this Author the application of Norwich principle is getting more frequent and it does not constitute an exception anymore, see *Ibidem*, 464 ff.

[169] ABRAMS, MCGUINNES, *Canadian Civil Procedure Law*, cit., 1089-1090. See also M. YIU, *A New Prescription for Disclosure: Reformulating the Rule for* Norwich *Order*, 65 U. Toronto Fac. L. Rev. 41, 44 ff. (2007) [YIU]. See *infra* for further details.

[170] *Telus's written representations*, 12.

[171] *Telus's written representations*, 3.

[172] It seems that Telus did not think that the balance would have considered users' rights, rather than ISPs' interests.

[173] *Telus's written representations*, 15.

disclosure by plaintiffs wishing to pursue civil actions" and that a high threshold test should be the appropriate one[174].

In particular, CIPPIC acknowledged that the letter of Rule 233 seemed to request a low threshold, but that at the same time the order was discretionary and this had led other courts to consider several relevant factors, including privacy of non-parties. The memorandum considered the *Irwin Toy v. Doe* case[175], where the Ontario Supreme Court of Justice granted the discovery of a non-party ISP in a case of defamation, holding that the test to be applied was whether the plaintiff had shown a *prima facie* case of defamation[176]. Usually in injunction cases a different test was applied, the so called "serious question to be tried" test[177]. This would require the judge to reach a conclusion "on the basis of common sense and an extremely limited review of the case on the merits"[178].

CIPPIC questioned the applicability of *Irwin Toy* to *BMG*. In the Ontario case no one appeared on behalf of the alleged defendant and even the non-party ISP did not appear or oppose the motion. Since defamation is a well-established tort action, it was quite clear that the plaintiff had been defamed, contrary to what happened in *BMG*. So the Court did not explain the meaning of the *prima facie* standard and did not provide an analysis to support its conclusion that in order to obtain disclosure plaintiff should demonstrate a *prima facie* case[179].

Then CIPPIC went on to address the core issue of the process, which is the privacy concern. In the intervener's view, since fundamental privacy values were at stake, a high threshold test would have been required. In a modern society people

[174] CIPPIC's memorandum of argument is available once again at http://www.cippic.ca/documents/file-sharing-lawsuits/Memorandum_final_12pt.pdf [*CIPPIC's memorandum*].
[175] *Irwin Toy Ltd. v. Doe*, [2000] O.T.C. 561 [*Irwin Toy*].
[176] *Irwin Toy*, par. 12.
[177] While the rules of procedure provide the way in which injunctions can be sought, the standard with which they are granted is a matter for judicial discretion. To guide judges there is a three-part test, developed in a British decision of the House of Lords, that is *American Cyanamid Co. v. Ethicon Ltd.*, [1975] A.C. 396 (H.L.). These three steps are: a) is there a serious question to be tried?; b) will the applicant suffer irreparable harm if the injunction is refused?; c) does the balance of convenient favour an injunction?. The first of the three parts is the one that can replace the "strong *prima face* case", and requires the applicant demonstrates only that there is a serious question being tried and the claim brought is not frivolous or vexatious. It is a lower standard than the *prima facie* case, and therefore judges tend to use the latter one when, for example, granting the injunction would make proceeding to trial pointless. For a better explanation see WALKER, SOSSIN, *Civil Litigation*, cit., 231 ff; ABRAMS, MCGUINNES, *Canadian Civil Procedure Law*, cit., 886 ff; A. ZUCKERMAN, *Zuckerman on Civil Procedure*, London, 2006, 308 ff.
[178] *CIPPIC's memorandum*, 5.
[179] *CIPPIC's memorandum*, 5.

know that in some situations they can count on a reasonable expectation that their data will not be divulgated and will be protected[180]. This important conception of privacy has been recognized by the Canadian government with the enactment of PIPEDA, as well as by other provinces, which at the time of the case had already passed their private sector data protection legislation[181]. And the Supreme Court of Canada has recognized a right to privacy inherent in sections 7 and 8 of the Charter of Rights and Freedoms, since respect for privacy is a basic part of people's freedom[182].

CIPPIC touched also upon the issue of online anonymity. Given the potential of the Internet as a forum for freedom of expression, anonymity works as a catalyst since it permits speakers to give voice also to unconventional or unpopular ideas, without fears of embarrassment or harassment. In this case, the Court would have ordered the disclosure of a user's information, the action subsequently commenced by CRIA could have made public other information regarding the same user, whose behaviour on the Web she thought was covered by anonymity. In some cases this could create significant embarrassment and also an irreparable harm to the user, with a corresponding chilling effect on free speech and online activity[183]. In *Irwin Toy,* the Court recognized the value of online anonymity: "[i]mplicit in the passage of information through the internet by utilization of an alias or pseudonym is the mutual understanding that, to some degree, the identity of the source will be concealed. […] [S]ome degree of privacy or confidentiality with respect to the identity of the internet protocol address of the originator of a message has significant safety value and is in keeping with what should be perceived as being good public policy"[184].

CIPPIC acknowledged that privacy online cannot be absolute, but that at the same time plaintiffs should not be allowed to uncover the identity of users based only on mere allegations. Setting low threshold tests would permit plaintiffs to engage in "fishing expeditions" and abuse the judicial process. In order to support its request

[180] See *R. v. Dyment*, cit., par. 33.
[181] See Québec's *Act Respecting the Protection of Personal Information in the Private Sector*, British Columbia's *Personal Information Protection Act* and Alberta's *Personal Information Protection Act*, cit.
[182] *CIPPIC's memorandum*, 5-7. See *supra* for a brief explanation of the conception of privacy in the Charter.
[183] *CIPPIC's memorandum*, 7.
[184] *Irwin Toy*, paras. 10-11.

for a high threshold, the intervener listed some characteristics of the order sought. In particular, the fact that the order would be invasive, without previous notice to the defendants[185], will irremediably remove users' anonymity and breach PIPEDA principles. Furthermore, there was uncertainty as to whether the alleged users' conduct could constitute an infringement of CRIA's copyright[186].

Then CIPPIC made a comparison between the order asked by the plaintiffs and an "Anton Piller" order, which is an aggressive form injunctive relief in common law systems[187]. Named after a UK case on copyright infringement[188], this kind of order provides the right to search premises and seize evidence on an *ex parte* basis. More precisely, it orders the defender to allow the complainant to enter her property for searching, inspecting and, if the case, copying named records[189]. Its obvious aim is to avoid the destruction or removal of evidence by the alleged infringer. In the founding case the Court of Appeal held that even if it had the power to make such an order, this should be done only in a very limited range of circumstances[190]. Given the exceptionality of this order, the court set down a specific test with three essential pre-conditions:

a) there must be an extremely strong prima facie case;
b) the damage, potential or actual, must be very serious for the plaintiff;
c) there must be clear evidence that the defendant has incriminating documents or things in her possession and that there is a real possibility that she may destroy such material before any application *inter partes* could be made.

[185] Except for those already noticed by their ISP, such as Roger's users.
[186] *CIPPIC's memorandum*, 8-9.
[187] For an explanation and critic of Anton Piller orders and their application and evolution in Canada, with special attention to intellectual property enforcement, see N. LIPKUS, *A Tale of Two Remedies: Rationalizing the Anton Piller Order in Canada*, 19 Intellectual Property Journal 459 (2006), spec. 468 ff.
[188] *Anton Piller KG v. Manufacturing Processes Limited*, [1976] 1 All E.R. 779 (C.A.).
[189] ABRAMS, MCGUINNES, *Canadian Civil Procedure Law*, cit., 924 ff; WALKER, SOSSIN, *Civil Litigation*, cit., 239-240. See also MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, cit., 624 ff. and VAVER, *Copyright Law*, cit., 259 ff.
[190] The court made clear that this was not a search warrant, but that it was just a way to bring pressure on the defendant to give permission, actually ordering her to give this permission, see *Anton Piller KG v. Manufacturing Processes Limited*, cit., 782-783.

Therefore this kind of order should be granted only when a normal process of the law would be frustrated if some immediate protection was not available to the requesting party[191].

CIPPIC argued that both in orders under Rule 233 and in Anton Piller orders a test balancing defender's privacy against the needs of the plaintiff is required. The similar degree of invasiveness suggested the application of a similar threshold as well[192]. Citing older intellectual property cases, the intervener explained that in order to meet the high standard required for an Anton Piller order, "the copyright or trade mark rights which are asserted must be clearly identified" and that the "applicant's rights to the intellectual property being asserted must also be clearly demonstrated"[193]. Plaintiffs should also be required to show clear evidence of the alleged infringement. Furthermore, when a case is unlikely to proceed to trial if an injunction is granted, court should engage in a more deep review of the merits of the claim. CIPPIC feared that once the information has been revealed, CRIA would have settled, given the enormous time and money costs for the defendants. This would have justified a more extensive analysis of plaintiffs' claims, to assure that they met a high standard[194].

Taking its observations into account, CIPPIC tried to sketch what test under Rule 233 would be appropriate in the particular case, listing a number of detailed questions that the court should have answered to understand the viability of the order[195]. The first question concerned the showing of a strong *prima facie* case. According to CRIA's statement of claim, defendants "(i) distributed to such an extent as to affect prejudicially the owner of copyright and (ii) possessed for the purpose of doing the things referred to in paragraph (i) unauthorized copies of the Sound Recordings that the defendants knew or should have known infringe copyright or would infringe copyright if they had been made in Canada by the

[191] *Anton Piller KG v. Manufacturing Processes Limited*, cit., 784. Given how much this order would be invasive, the Supreme Court of Canada set down a number of detailed guidelines to govern the preparation and the execution of the order, as well as the procedure to be followed after the search, see ABRAMS, MCGUINNES, *Canadian Civil Procedure Law*, cit., 933 ff. It seems that courts have begun to make such orders in cases where the need for it was far from self-evident, see *Ibidem*, 925.
[192] *CIPPIC's memorandum*, 9.
[193] *Fila Canada Inc. v. Doe (T.D.)*, [1996] 3 F.C. 493, paras. 9-10.
[194] *CIPPIC's memorandum*, 11.
[195] For the list of questions see *CIPPIC's memorandum*, 13.

person who made them"[196]. In CIPPIC's opinion, any reproduction of copyrighted material made by the defendants was legal under section 80 of the *Copyright Act*, which, as seen, contemplates copying for private use. This would make "downloading for private use onto audio recording media" legal in Canada, as long as it is undertaken in accordance with the just mentioned section[197].

In particular, according to CIPPIC's reconstruction of the facts, P2P users do not upload, given that "uploading" should mean transmitting from a computer to another[198]. In fact users do not send files to other users or to an entity; they just allow files to be copied by another user, who is a downloader. There was no evidence that a user actively and intentionally sent files to other people, which would be the needed activity in order to talk of "uploading". Neither there was evidence that users were aware that they were allowing file sharing and, in any case, the simple fact that a user let others downloading from her computer did not mean that the download actually took place. Under section 80 downloading and reproduction are legal as long as they are not made for the purposes listed in the same section. In this case CIPPIC stated that users had no "purpose" of "distributing", because purpose would have meant the consciousness of the act of distribution[199].

Furthermore CIPPIC pointed out that, as opposed to American law, distribution is not an exclusive right under Canadian copyright legislation, since, as previously explained, it is not listed among the sole rights contemplated in Section 3. It was contemplated in section 27 of a previous version of the *Copyright Act*[200], under the title "secondary infringement", stating the possibility that infringement could be made through distribution "to such an extent as to affect prejudicially the

[196] See CRIA's statement of claim at page 3. The statement is available at http://www.cippic.ca/documents/file-sharing-lawsuits/CRIAStatementofClaim.pdf [*CRIA's statement of claim*].
[197] *CIPPIC's memorandum*, 15.
[198] *Entry: Uploading,* SOOKMAN, *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions*, cit., 395.
[199] *CIPPIC's memorandum*, 15.
[200] It is now inserted under Criminal Remedies, Section 42(1)(c) of the Copyright Act punishes: "Every person who knowingly […]distributes infringing copies of a work or other subject-matter in which copyright subsists, either for the purpose of trade or to such an extent as *to affect prejudicially the owner of the copyright*".

owner of the copyright"[201]. Distribution is also mentioned in section 80 as a limitation to copy for private use. The only cases where there was a "distribution" of file in the online context under *Copyright Act* involved the uploading to a Bulletin-Board System (BBS)[202]. In those cases there was a deliberate and intentional action of uploading the files, which could be then "widely dispersed"[203]. Even if defendants had distributed plaintiffs' copyrighted works, according to the intervener the distribution had not caused any arm as "to affect prejudicially the owner of the copyright"[204].

CIPPIC held that plaintiffs were trying to assert an exclusive right to "make available". As noted earlier in this chapter, this exclusive right is included in the WIPO Treaties of 1996, which had not been implemented at the time of the BMG case. Moreover, the Copyright Board had ruled that "[a] work is communicated not when it is made available, but when it is transmitted. Those who argue that a work is communicated when it is made available, for example, by storing it on a host server where it can be accessed by members of the public, rely both on an international treaty and on Canadian court decisions"[205]. However these treaties were not binding in the particular case, since, as said, Canada had signed but not ratified them yet. In his affidavit, Millin described peer-to-peer by using the sentence "make those files available", which basically confirmed the idea that plaintiffs' were trying to apply WIPO language and regulation to the case[206].

In addition to the claims directed to the alleged infringer, plaintiffs stated that the infringement could have taken place with the authorization of the person holding the account, who could be therefore held responsible for activities made by

[201] See Part III of the Copyright Act version existing when the case was decided: "Infringement of Copyright and Moral Rights and Exceptions To Infringement", Section 27(2)(b).
[202] A bulletin board offers both electronic mail services and newsgroups, that is basically an e-mail directed to an entire community and not to a private recipient. It can be thought as the electronic equivalent of a bulletin board commonly found at a workplace or at home. A computer bulletin-board system is a computer program which simulates a bulletin board, by allowing users to post messages, read and delete existing ones. They can be used to transmit information to closed or open groups. See *Entries: Bulletin Board* and *Bulletin-Board System*, SOOKMAN, *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions*, cit., 38 ff.
[203] *CIPPIC's memorandum*, 18. The cases cited by CRIA involved alleged criminal activities, see *R. v. Pecciarich*, [1995] O.J. No. 1004 and *R. v. J.P.M*, [1996] N.S.J. No. 124.
[204] Section 27(2)(b) of the previous version of Copyright Act as above mentioned.
[205] *CIPPIC's memorandum*, 19, citing SOCAN Statement of Royalties, Public Performance of Musical Works 1996, 1997, 1998 (Tariff 22, Internet) (Re) 1 C.P.R. (4th) 417 at 448, available at: http://www.cb-cda.gc.ca/decisions/1999/19991027-m-b.pdf [*Tariff 22 CB*].
[206] *CIPPIC's memorandum*, 20.

others using her account. But the Supreme Court of Canada, in the famous decision *CCH,* stated that "courts should presume that a person who authorizes an activity does so only so far as it is in accordance with the law"[207]. This principle could be well applied also to BMG case: an account holder cannot control the activities which take place in her account. *CCH* did not contain any provision under which an account holder should actively intervene to control the account. This is particularly true in this case, since a person's computer could be sharing files even if the same person closed the file-sharing software, meaning that this person could not control her computer even if she wanted to. Furthermore, since more than one computer may be using the same IP address, as explained by the respondent ISPs, the holder of the account cannot possibly control what is happening on each computer[208].

Finally CIPPIC's memorandum addressed the question of linking an IP number to an account and to an alleged infringer. "An IP address is analogous to a place […]. However, an IP address cannot definitely establish the identity of the actual person involved in the complained of activity any more than a simple street address can necessarily identify the person who actually committed a wrong doing at that address"[209]. Therefore even if the plaintiffs were able to effectively link IP addresses to account owners at a particular time, this would not mean that they would have found the real infringer (assuming that the owner would be a person and not a company or another organization)[210]. Plaintiffs should have born the burden of proving that the defendants were the persons who they alleged to be the infringers or that, at least, the defendants were vicariously liable for somebody else's infringement. Trying to obtain defendants' information and force them into litigation only to find out if they were or not the correct party would have been in contrast with the Charter's values and rights[211].

[207] *CCH*, 342. For more details on this case see *infra*.
[208] *CIPPIC's memorandum*, 20-21.
[209] *CIPPIC's memorandum*, 22-23.
[210] We should anyway remember that some of the respondents raised many doubts on the possibility of linking IP addresses and account holders; see *supra*.
[211] *CIPPIC's memorandum*, 23.

f) EFC's memorandum of argument

Likewise CIPPIC, Electronic Frontier Canada (EFC)[212], asked and obtained the possibility to intervene and serve a written memorandum.

EFC opened its memorandum explaining the risks connected to the possibility that the wrong people were identified through the matching of IP and account holders[213]. Then it addressed the question of the correct test to be applied in deciding on the disclosure. The judicial exercise of discretion should have involved the balancing of competing public interests against the disclosure. In particular, according to EFC, evidence should be excluded when "its prejudicial effect outweighs its probative value"[214].

The intervener then referred to a Canadian Supreme Court decision, which stated that disclosure would be contrary to the interest of justice if privilege is established and which applied the following test:

a. "The communications must originate in a confidence that they will not be disclosed;
b. This element of confidentiality must be essential to the full and satisfactory maintenance of the relation between the parties;
c. The relation must be one which in the opinion of the community ought to be sedulously fostered;
d. The injury that would inure to the relation by the disclosure of the communications must be greater than the benefit thereby gained for the correct disposal of litigation"[215].

As sustained by CIPPIC, EFC stated that the Does had an expectation of privacy about their information. Given the possible unreliability of the data eventually disclosed, the prejudice to the defendant would, in EFC's opinion, outweigh the probative value of obtaining the information[216]. The plaintiffs should have proved that the information was relevant, that is "where it relates directly to the fact in issue, but

[212] "Electronic Frontier Canada (EFC) was founded to ensure that the principles embodied in the Canadian Charter of Rights and Freedoms remain protected as new computing, communications, and information technologies are introduced into Canadian society", see www.efc.ca.
[213] *EFC's memorandum of argument*, 4-5, available at http://www.cippic.ca/documents/file-sharing-lawsuits/document-archives.html [*EFC's memorandum*].
[214] *EFC's memorandum*, 7, citing the House of Lords case *British Steel v. Granada Television*, [1981] 1 All ER 417.
[215] *Slavutych v. Baker*, [1976] 1 S.C.R. 254.
[216] *EFC's memorandum*, 8.

also where it proves or renders probable the past, present or future existence (or non-existence) of any fact in issue". Since the evidence was unreliable, the intervener argued that CRIA had a greater obligation to ensure that the privacy rights of the users were not needlessly violated and to prove that it was relevant to the question of the alleged copyright infringement[217].

In order to address this problem, EFC listed some questions that the Court should have itself answered before ordering the disclosure[218]. Furthermore, the intervener recommended that, in case the Court had granted the order, it would have imposed some conditions to ensure the rights of Does to be protected as much as possible, with particular regard to their due process right[219].

g) CRIA's written representations

In its written representations[220], CRIA cited the so-called *Norwich* principle, as also other actors in the BMG pleadings had also done. As said, *Norwich* stated that a person who is involved in the wrongful act of another, even if she has no fault, is under a duty to assist a person who was injured by this wrongful act by giving full information to disclose the identity of the wrongdoer. The plaintiffs argued that, following this principle, ISPs should have disclosed the requested information, has the relief been sought either by way of an equitable bill of discovery[221] or through third party production under Rules 233 and 238. The order would have been the only opportunity for the recording companies to obtain the enforcement of their

[217] *EFC's memorandum*, 9.

[218] The questions are the following: EFC presented a list of questions the Court should have asked itself before ordering the disclosure: "1. Is the information sought private information? If so, should the privacy of the Users be violated? 2. Does privilege attach to the information sought by the Plaintiff? If so, the information should not be disclosed. 3. Have the Plaintiffs established a *prima facie* cause of action? 4.Does the probative value of the disclosure sought outweigh its prejudicial effect? 5. Is the evidence relevant? Is the court satisfied that the Users are one and the same as the Unnamed Defendants?" *EFC's memorandum*, 9-10.

[219] *EFC's memorandum*, 10-11.

[220] Available at http://www.cippic.ca/documents/file-sharing-lawsuits/Plaintiffs_Submissions_March_12.pdf [*CRIA's written representations*].

[221] "This remedy permits a court, acting through its equitable jurisdiction, to order discovery of a person against whom the applicant for the bill of discovery has no cause of action and who is not a party to contemplated litigation", *Glaxo Wellcome*, par. 20. According to BLACK, *Black's Law Dictionary*, cit., 173, a bill of discovery is a "bill in equity seeking disclosure of facts within opposing party's knowledge".

copyright[222]. With regard to this, the plaintiffs held that the test to be applied was whether they had a *bona fide* case of infringement or not[223].

Addressing the issue of privacy, CRIA stated that in the particular case there was no expectation of privacy and that the disclosure of the sought information would have not breached PIPEDA, given that the Act explicitly authorizes disclosure of personal information in the cases provided under section 7(3)(c). Further, the plaintiffs held that subscribers had consented to the disclosure of their information when they agreed to the terms of services with their ISP[224]. CRIA argued that ISPs were the only practical source of information available and that despite the differing opinion of the ISPa, the data maintained by the providers would be reliable[225].

With regard to showing the *prima facie* case, CRIA asserted that they had filed "uncontradicted evidence" of either copyright ownership or exclusive right to copyright to certain sound recordings. In particular, they maintained that the evidence could show that individuals had copied the mentioned sound recording to publicly shared computer directories, in this way making recording available for copy, transmission and distribution to potentially millions of other file-sharers. In plaintiffs' mind this was sufficient to show a *prima facie* case of copyright violation[226].

CRIA then analyzed in detail the test needed to obtain the order of disclosure, relying on the landmark *Glaxo Wellcome*. According to this analysis, the criteria for issuing a bill of discovery contemplated three requirements:

1) the applicant should establish a *bona fide* claim against the alleged infringer[227];

2) the applicant has to share some sort of relationship with the respondent through the wrongdoing;

3) the person from whom the information is sought must be the only practical source of information available.

---

[222] *CRIA's written representations*, 3.
[223] *CRIA's written representations*, 6.
[224] *CRIA's written representations*, 6.
[225] *CRIA's written representations*, 5-6.
[226] *CRIA's written representations*, 7.
[227] *CRIA's written representations*, 9-10. In CRIA's view "bona fide" claim was just the same of "prima facie". CRIA's precise words were "[t]he applicant must establish a bona fide (*i.e. prima facie*) claim against the alleged wrongdoer" (emphasis added).

The recording industry then acknowledged that in deciding whether to grant the order, the court should have taken into account the public interest both in favour of and against disclosure. CRIA asserted that, on the one hand, the disclosure was the only way to sue the infringers and, on the other hand, there was nothing that could weigh against giving CRIA the opportunity to sue. As seen above, under Rule 233(1) a federal court has the power to order a non-party the production of a document, if this document is relevant and its production could be compelled at trial. Given that ISPs had possession of the relevant information and that this information could have been compelled at trial, CRIA held that the court should have ordered the disclosure[228].

The claimant then moved to the analysis of Rule 238(1), which, as mentioned, permits a party to an action to examine for discovery any person who is not a party to the action, when this person might have information on an issue in the action. Again, CRIA listed the factors a court should consider in order to grant the discovery:

a) the person may have information regarding an issue in the action;
b) the party has not been able to obtain the information informally from the same person or from another source or by any other reasonable mean;
c) it would be unfair not to allow the party the opportunity to question the person before trial;
d) the questioning will not cause undue delay, inconvenience or expense to the person.

The applicant must show that the evidence cannot be obtained from anyone else. Moreover the applicant should prove that, despite the fact that she did not obtain the information needed, she actually tried to obtain it informally by the same person or from other sources. CRIA adduced that it had asked the ISPs to voluntarily provide the information, but that none of them did. Therefore, since in the plaintiffs' opinion all the requirements listed above were met, they held that the Court should have granted the motion. In addition, CRIA cited previous cases in which courts had granted the discovery of the information related to an IP address. In particular, it referred to *Irwin Toy*, in which, as mentioned before, the Ontario Supreme Court of

[228] *CRIA's written representations*, 10.

Justice granted the discovery of a non-party ISP in a case where the plaintiff sought to identify the person who defamed his company through an e-mail. After discussing some important public policy issues, that Court concluded that the test to be applied was whether the plaintiff had shown a *prima facie* case of defamation[229]. CRIA held that the test applied in *Irwin Toy* would be appropriate for this case and that only when seeking an Anton Piller order should a party demonstrate a higher "strong prima facie" test[230].

CRIA then suggested that disclosure of the identity of customers linked to an IP address was routinely sought and routinely provided under court orders as well. As a support for its request CRIA affirmed that it had demonstrated

- the existence of "a *prima facie* or *bona fide* case" of infringement[231];
- the existence of a relationship between the ISPs and the alleged infringers;
- the fact that ISPs had documents and information about those infringers;
- that there were no other practical source of information;
- that there was the necessity of this information for CRIA to proceed;
- that such information and documents would have been compellable at trial and useful to the plaintiffs' case;
- the fact that neither the ISPs nor the alleged infringers would have any interest to outweigh the ISPs duty to disclose the identity of the alleged infringers themselves[232].

After affirming to be absolutely entitled to the discovery, CRIA examined in more detail some specific points, first of all the privacy issue.

In the recording industry's opinion, the case was just "a matter of private law" and the Charter was not applicable, since government actions were totally absent. More precisely, even if in private law matters the common law should be interpreted in light of the Charter's principles, this did not mean to import into private litigation the analysis usually applied in cases regarding governmental actions[233]. The consequence of this reasoning would have been that article 8 of the

[229] *Irwin Toy*, par. 12.
[230] *CRIA's written representations*, 13.
[231] Again, CRIA was equalizing *bona fide* and *prima facie* case.
[232] *CRIA's written representations*, 13-14.
[233] Citing *Hill v. Church of Scientology of Toronto*, [1995] 2 S.C.R. 1130 and *R. v. Fegan,* [1993] O.J. No. 733.

Charter was not applicable, since, according to CRIA's view, it protects citizens only against invasion of the State when there is a reasonable expectation of privacy[234].

The recording industry went further, taking into consideration also the impact of PIPEDA. Section 4.3 of Schedule 1 states that sometimes the knowledge and consent of the individual to whom the information are related could be inappropriate[235]. Moreover section 7(3)(c) provides an important exception to the rule in the just mentioned section 4.3: "(3) For the purpose of clause 4.3 of Schedule 1 […] an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is […] (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records"[236].Plaintiffs' held that this section was applicable in their case, given that the purpose of CRIA's motion was to obtain an order for the production of information from the respondents[237].

According to the recording industry, the defendants should have not any expectation of privacy. In particular, if their data were maintained as a part of a commercial relationship, the nature of the relationship itself had to be examined. If the information was not "personal and confidential", then there could not be expectation of privacy. To understand the relationship between ISPs and their customers, it was necessary to investigate the so-called "terms of agreement" that normally establish the conditions of the service a user subscribes. CRIA submitted that these terms notified subscribers that their information could be disclosed if they engaged in prohibited activities, including the dissemination of material that violates

[234] Referring to *R. v. Plant*, [1993] 3 S.C.R. 281, paras. 23-24.
[235] PIPEDA – 4.3 Principle 3 – Consent: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information".
[236] PIPEDA – Section 7(3)(c).
[237] *CRIA's written representations*, 15.

copyright and the use of P2P file-sharing systems. Since apparently all the necessary consents had been obtained from the subscriber, the disclosure requested by CRIA could be ordered without problems. Given the existence of PIPEDA section 7(3)(c) and of the accepted terms of use, plaintiffs argued that the Does could not have had a reasonable expectation of anonymity, especially in light of such an evident *prima facie* case of copyright infringement against them[238].

Then, in response to the concerns of CIPPIC regarding the chilling effect on freedom of speech, CRIA argued that the "likelihood that members of the public would be able to trace the defendant's activities at large on the Internet based solely on the KaZaA user names and the IP addresses disclosed by the plaintiffs is remote due to the dynamic way IP addresses are reassigned, the limited utility KaZaA pseudonyms have in identifying the defendants and the ability of users change pseudonyms"[239].

The applicants quoted the CIPPIC paper, where the intervener admitted that privacy interests of the defendants were not limitless and that privacy online is not absolute, for they cannot cover activities which violate the rights of other people. The interests that the Does could have in keeping their anonymity were to be balanced against the interests of CRIA in enforcing its copyright. In the plaintiffs' view, users' privacy could not outweigh ISPs' duty to disclose the information asked for[240].

In order to support its claim of infringement, the recording industry then described how file-sharing works. According to its explanation, through peer-to-peer programs a user could […] "transmit exact copies of files from the subscriber's computer to another via the Internet"; therefore "[f]ile sharing is not mere downloading". The alleged infringers "offered files for copying, transmission and distribution to others via peer-to-peer services. They have stored those files in special, shared directories on the subscriber's directory that they have opened to other users to view and access on the Internet using the file-sharing service". In a somewhat different description of how peer-to-peer works, if compared to the one advanced by CIPPIC, CRIA held that when a user copies a file into a shared directory of her computer, connects to the Internet and runs the application, she

[238] *CRIA's written representations*, 17-18.
[239] *CRIA's written representations*, 18.
[240] *CRIA's written representations*, 19.

authorizes a massive number of other users to search her computer "and also authorizes, facilitates and participates in copying and distribution of copies of that sound recording to other users over the Internet"[241].

Still in order to defend its claim, CRIA explained that MediaSentry had collected evidence that the alleged infringers had copied plaintiffs' records to the mentioned shared folders and allowed the copying, transmissions and distribution from their computers. To ascertain this, MediaSentry had itself downloaded and stored samples of the recording files placed in the alleged infringers' shared directories. This would have been a sufficient proof that the Does had *made available* these sound recordings to be copied, transmitted and distributed[242].

In its concluding remarks, CRIA invoked the application of Sections 18 and 27 of the Copyright Act, holding that Does had violated these provisions as follows:

a. "reproduction of sound recordings by the alleged infringers (s. 18(1) and s. 27(1));
b. authorization of the reproduction of the sound recordings (s. 18(1) and s. 27(1));
c. distribution of unauthorized copies of the sound recordings to such an extent as to affect prejudicially the plaintiffs (s. 27(2)(b)), and
d. possession of unauthorized copies, which the alleged infringers knew or ought to have known were infringing, for the purpose of distribution, as set out above (s. 27(2)(d))"[243].

The plaintiffs' written response analyzed each of the four mentioned behaviors.

For what reproduction was concerned, CRIA addressed the issue of the applicability of the exemption provided by Section 80 of the Copyright Act, regarding, as already said, copies for private use. Citing a decision of the Copyright Board, CRIA illustrated that exemption under Section 80 "expressly excludes selling, renting out, exposing for trade or rental, distributing, communicating to the public by telecommunication, or performing in public the copy made. […] distributing this same copy to friends online is prohibited"[244]. The inclusion of the recording files in a shared

[241] *CRIA's written representations*, 21.
[242] As held by CIPPIC, CRIA made reference to "make available" their sound recordings, using the words of WIPO Treaties; see *supra*.
[243] *CRIA's written representations*, 26-27.
[244] *Private Copying 2003-2004*, 20.

directory would have been an act of distribution and the consequential transmission of copies online would have been a communication to the public. Therefore, these actions would have excluded the applicability of the exemption of private copying, given that Section 80(2) provide that subsection (1) does not apply if the copying is done for "the purpose of either distributing (subs. (b)) or communicating to the public by telecommunication (subs. (c))"[245].

To explain the depth of the word "communication", the recording industry relied on another decision of the Copyright Board, the well-known *Tariff 22*: "a work is communicated to the public even if it is transmitted only once, as long as it is made available on a site that is accessible to a segment of the public"; "[t]he fact that the communication is automated is irrelevant"[246]. According to the same decision, authorization is a "separate protected use under the Act"[247]: "[b]y making a work available, a person authorizes its communication"[248]. Therefore, in CRIA's opinion, the fact that the Does had placed the files in their computers' shared folder meant that they were authorizing the communication of those files[249]. CRIA cited also *CCH*, where it was specified that the term "authorization" has to "be understood in its strongest dictionary meaning, namely, 'give approval to, sanction, permit, favour, encourage'"[250].

With regard to distribution, CRIA referred to a case decided by the Nova Scotia Court of Appeal[251]. As previously mentioned, the case pertained to the distribution of copyrighted programs on a bulletin board. The recording industry stated that the Nova Scotia case and the case at bar could be compared, because they were "functionally equivalent": "[i]n a peer-to-peer file sharing context, the file sharing application on the user's own computer and the user's own shared file directory act as a bulletin board". The fact that users had made files available, copied

[245] Remember on this point CIPPIC argued that users did not distribute "on purpose", since the file-sharing program allows the transmission to other users, even without knowledge of the computer owner; see *supra*.
[246] *Tariff 22 CB,* 37.
[247] *Tariff 22 CB*, 44.
[248] *Tariff 22 CB*, 26.
[249] *CRIA's written representations*, 30.
[250] *CCH*, 361.
[251] *R. v. J.P.M.*, *cit*.

them and transmitted to (at least) MediaSentry meant that they had distributed the recordings[252].

Finally, in the plaintiffs' mind, possession could be easily proved, since the sound files were found in users' shared directories[253].

3.3.2 Previous cases on which the Courts relied

In deciding the outcome of *BMG v. Doe*, the Federal Court cited a number of leading cases, sometimes considered also by the parties. In the following pages, I shall briefly summarize them, for a better understanding of the solution given in that case.

a) Norwich Pharmacal v. Customs and Excise Commissioners

The *Norwich* principle gives Courts power to order disclosure before proceedings have started and against a non-party[254].

Norwich is a case decided in United Kingdom and pertains to a patent infringement by illegal importations. Norwich Pharmacal was an American corporation that owned a patent, for which Smith Kline and French Laboratories Ltd. were the subsidiary and licensee. In particular the patent concerned a chemical compound called "furazolidone". This was related to poultry food, giving the birds a measure of protection against specified microbes.

The claimants had a strong belief that somebody had illicitly imported the same compound, but they did not know who these illegal importers were, thus preventing them from suing the alleged infringers for patent violation. Therefore, Norwich decided to sue the Customs and Excise Commissioners, given that from the moment the goods entered the port until the time they were taken by the consignee, they were under the control of the commissioners. Furthermore, the importer had to fill in the form of entry, giving the name of the importers and some other information on the good. This meant that the commissioners had documents which could identify

[252] *CRIA's written representations*, 30-31.
[253] *CRIA's written representations*, 32.
[254] UK Civil Procedure Rule 31.17 which provides the possibility of obtaining information from non-party and Rule 31.18, that preserves the court's pre-CPR powers to order disclosure before proceedings have started, as in the case of a Norwich order, see D. BASU, *Obtaining disclosure from non parties*, 2 Journal of Personal Injury 198, 200 (2005).

the infringers and which could provide evidence related to the importation of material infringing Norwich's patent. The problem was that this information was confidential and the Customs did not publish it at all. The claimants sought an order for disclosure of the names and addresses of the infringers, basing their claim on the "equitable right to file a bill for discovery".

Originally the plaintiff sued the commissioners alleging that they were themselves guilty of infringing the patent, either as principals or as parties and that, in that context, they could have been obliged to discover the information sought by Norwich. But the Court of Appeal concluded that the claimant had no reasonable cause of action, which in turn meant no right of discovery[255].

The House of Lords had a different approach. Indeed, no disclosure should have been ordered since this would have infringed the "mere witness" rule. This rule provides that information might not be obtained by discovery from a person, if this person could be compellable either to give oral testimony as a witness or on a *subpoena duces tecum*, unless there is a separate cause of action against the person from whom the information is sought on which could be relied upon. The rationale of this rule is that the testimony would be available by other means, either in an action already in progress or in an action that could be brought[256].

Furthermore, the appellants were seeking from the commissioners only the names of the alleged infringers and did not seek discovery of documents. According to them, this was a distinction between *Norwich* and previous cases on discovery issues[257].

The House of Lords took a different approach, pointing out that this rule could not be applied in a case where, without the requested information, the trial for the wrongdoer would never take place. Indeed, the purpose of the mere witness rule is not to prevent, but only to postpone the recovery of the data sought[258]. Given that no trial could be started unless the infringers were identified, the House of Lords granted the order. Nevertheless this relief would have not been available against every bystander. In fact, the commissioners were in a special position, since the

[255] K. LAROCHE, G.J. PRATTE, *The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation*, 18 Canadian Intellectual Property Review 117, 119 (2001).
[256] HOLLANDER, *Norwich Pharmacal takes wings*, cit., 458.
[257] See *Norwich,* 152.
[258] See *Norwich,* 174.

infringing goods were under their control. The commissioners had therefore been innocently mixed up in the importers' tort. According to Lord Reid, the respondents were "in an intermediate position. Their conduct was entirely innocent; it was in execution of their statutory duty. But without certain action on their part the infringements could never have been committed"[259]. Then, Lord Reid laid down the core principle of Norwich Pharmacal: "[i]f through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrong-doing he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrong-doers"[260]. It did not matter whether the person got mixed up voluntarily or because of her duty. The disclosure was available as long as an individual had a connection with the wrongdoing other than being a mere spectator of it and when possessing some documents relating to the wrongful action[261].

Furthermore, Lord Reid held that the disclosure should have been weight against public policy considerations that could prevent it. Respondents justified their non-disclosure with two arguments: first, they said that such disclosure would or might impair or hamper the efficient conduct of their duties, and; second, that that disclosure could be prejudicial for those whose identity would be disclosed. Lord Reid said that the information was in no way confidential. He also stated that he could not believe that other traders would have been hurt by this disclosure, given that it was related to wrongdoers. As for the second reason, Lord Reid thought that it was a more difficult matter, but that in the particular case the possibility that those individuals being innocent was "remote"[262]. Finally, Lord Reid stated that it was appropriate for the person seeking the information to reimburse the innocent person for the costs of searching the information[263].

Other Lords expressed their concern with this application of the bill of discovery. The reason of Lord Cross, in particular, set out the criteria that a court might follow in ordering discovery:

---

[259] *Norwich,* 174.
[260] *Norwich,* 175.
[261] P. COX, *Evolution or revolution? Norwich Pharmacal orders over the last 20 years*, Trademark World, 2004, 41 available at http://www.sjberwin.com/Contents/Publications/pdf/102/220206124930.pdf.
[262] *Norwich,* 176.
[263] *Norwich,* 172. As reported, all the respondent ISPs in BMG were concerned about the costs of the information sought and disclosure.

- the strength of the applicant's case against the alleged tortfeasor;
- the relation subsisting between the alleged wrongdoer and the respondent;
- whether the information could be obtained from another source;
- whether giving the information would put the respondent to trouble which could not be compensated by the payment of all expenses by the applicant.

These requirements, which are those applied also by Canadian courts, were necessary because, in the opinion of Lord Cross, the "new" application of the equitable disclosure could have been the "thin edge of the wedge" and open the possibility to "fishing requests" by plaintiffs that wanted to collect evidence for further cases[264].

The rationale for this kind of order is the idea that it would be unjust for a person who facilitated (or was anyway involved in) a wrong against another to deny the victim information she requires in order to vindicate the tort suffered[265].

Nowadays, with *Norwich* orders UK courts are willing to override the protection offered on data by the law of confidence or data protection law. The *Norwich* principle has been applied in many cases; each of them has extended the principle and broadened the criteria for its application[266]. More recent cases showed that through this order one can now obtain full information about an alleged wrongdoer, including documentation to enable the claimant to pursue those wrongdoers also outside UK[267]. Today, the *Norwich* order is used in UK also for the purpose of enforcing copyright against file sharing, in cases like those analyzed in this work where the plaintiff needs to find out the identity of the person behind the IP number[268].

---

[264] *Norwich,* 199. "*Norwich Pharmacal* does not give claimants a general licence to fish for information that will do no more than potentially assist them to identify a claim or a defendant", see J. O'HARE, K. BROWNE, *Civil litigation*, London, 2009, 506 also for further explanation of the functioning of the order, as well as ZUCKERMAN, *Zuckerman on Civil Procedure*, cit., 578 ff.

[265] ZUCKERMAN, *Zuckerman on Civil Procedure*, cit., 579. He further states that "the common thread running through these cases is that disclosure is necessary in order to enable a person to vindicate his rights and a sense of the injustice that would ensue if the court did not come to his assistance and order disclosure", see *Ibidem*, 581 ff. for a deeper explanation of Norwich orders.

[266] See LAROCHE, PRATTE, *The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation*, cit., 120, for a list of summarized cases in which the principle was applied.

[267] COX, *Evolution or revolution? Norwich Pharmacal orders over the last 20 years*, cit., 44.

[268] T. O'FLYNN, *File sharing: an holistic approach to the problem*, 17 Entertainment Law Review 218, 218 (2006), see also LAROCHE, PRATTE, *The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation*, cit., 122-123.

As seen, the *Norwich* case dealt with a problem of confidentiality. To be considered confidential the information requested has to be subject to a case-by-case analysis to qualify for common law privilege[269]. This privilege requires a court to apply the so-called "Wigmore test". This test implies that the following conditions must be met: "(1) the communications must originate in a confidence that they will not be disclosed; (2) this element of confidentiality must be essential to the full and satisfactory maintenance of the relation between the parties; (3) the relation must be one which in the opinion of the community ought to be sedulously fostered; and (4) the injury that would inure to the relation by the disclosure of the communications must be greater than the benefit thereby gained for the correct disposal of litigation"[270]. What matters for the scope of this work is with no doubt the fourth requirement, that is a plain balancing test. Normally, when there are only private interests at stake and no public ones, there is little possibility that the privilege would be granted[271].

As for Canada, the rules of civil procedure in more than one province have for many years contained provisions which permit discovery before starting a proceeding. This may be one of the reasons why this kind of order has not been frequently applied in the Canadian system[272]. The first Canadian court to adopt the principle of Norwich was the Federal Court of Appeal in the *Glaxo Wellcome*, which I shall now summarize.[273]

b) Glaxo Wellcome

Glaxo Wellcome is a case which is very similar to the Norwich case. Glaxo Wellcome PLC, one of the world's largest pharmaceutical companies, held two patents on a compound called RHCL. The company learned from reports published by Statistics Canada that a large quantity of the same compound had been imported by companies other than Glaxo or its authorized licensees. Glaxo made a request

[269] The information could also fall into a category of class privilege, but they are few and are not of our interests, see YIU, 65.
[270] YIU, 65. The test is named after the author of the book who proposed it, see J.H. WIGMORE, *Evidence in Trials at Common Law*, vol. 8, Boston, 1961, 527.
[271] YIU, 65.
[272] YIU, 43.
[273] LAROCHE, PRATTE, *The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation*, cit., 126.

according to the *Access to Information Act*[274] in order to obtain information concerning the importation. The request was denied, since the information was exempt from disclosure. Consequently Glaxo applied to the Department of National Revenue for disclosure of the names of the importers[275], but the minister rejected the application on the basis of the confidentiality of the information requested. Glaxo brought an application for judicial review.

The Federal Court of Appeal recognized that the equitable bill of discovery had a long history, but that the *Norwich* case had given it new importance. In delivering his opinion, Stone J. acknowledged that the case was very similar to *Norwich*. After revising the principles applied in the English case[276] and after solving the problem of the applicability of an equity remedy[277], the Judge analyzed whether the appellant in *Glaxo* satisfied the conditions for granting the relief sought.

Considering the Norwich principle, the Court stated that four different criteria should have been applied. These criteria, which are basically those listed by Lord Cross in *Norwich,* are:

a) the plaintiff must show a *bona fide* claim. The *ratio* behind this provision is trying to avoid actions for bill of discovery which are frivolous[278];
b) the plaintiff must share some relationship with the defendants. In Stone J.'s words this is "an alternative formulation of the principle that a bill of discovery may not be issued against a mere witness or disinterested bystander";
c) the person to whom the request is made must be the only practical source of information available;
d) the public interest against disclosure must be considered by the court before ordering the disclosure. As Lord Reid specified, the court should weigh the requirements of justice to the appellants against the argument of the respondent for not disclosing[279].

[274] Access to Information Act (R.S.C., 1985, c. A-1).
[275] Glaxo did so under Section 108(1) of the Customs Act, see *Glaxo Wellcome*, par. 7.
[276] *Glaxo Wellcome*, paras. 22-30.
[277] *Glaxo Wellcome*, paras. 31-43.
[278] YIU, 74, argues that Norwich orders should be limited to their initial scope of finding wrongdoers and not as a mean of pre-proceding discovery. This, in turn, would mean that the plaintiff's claim should be well grounded, but it would not need to be as high as a *prima facie* standard.
[279] *Glaxo Wellcome*, paras. 22-30.

In particular, as for the source of information, Glaxo had hired a private investigator and this, in motion judge's opinion, was the proof of the existence of another practical source of information. Stone J. disagreed, since there was a witness who stated that the private investigation led to totally unsatisfactory results, which in turn meant that this was not a practical option[280]. In the subsequent cases this criterion has been interpreted as related to the "efficacy" of the source of information. If other sources were available, but would not be an efficacious way to obtain the information, then the respondent would be a practical source[281]. Nonetheless, Stone J. specified that the mere non-existence of a practical alternative source of information was not in itself enough for granting the discovery[282].

For what the connection between the wrongdoer and the person from whom the information is sought, the concept of "being mixed-up" should be read as follows: the real issue is "whether the respondent's evidence is required in order that there be (or could be) a trial of allegations that, in the view of the court, warrant a trial"[283]. In such a case, the respondent is not a mere witness, but she is sufficiently "mixed-up".

With regard to the requirement listed under the letter d), the respondent argued that the information sought by the claimant was confidential. The Court in *Glaxo Wellcome*, pointing out the fact that the names of importers would have passed through many hands before reaching those of custom officials, said that these data were not particularly sensitive. Therefore, the public interest in ensuring that the appellant could pursue its concerns against the alleged infringers outweighed the public interest in maintaining the information confidential[284].

After the *Glaxo Wellcome* case, the doctrine of equitable discovery has become rooted in the Canadian system[285]. Canadian courts have applied the principle with elasticity, giving this remedy an investigative utility that is nonetheless subject to the above-mentioned criteria. In particular, according to Lord Cross's words and

[280] *Glaxo Wellcome*, paras. 45-46.
[281] *Alberta Treasury Branches v. Leahy*, [2000] A.J. No. 993, par. 157.
[282] *Glaxo Wellcome*, par. 58.
[283] LAROCHE, PRATTE, *The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation*, cit., 130.
[284] *Glaxo Wellcome*, par. 62.
[285] For other cases applying the same principle, see LAROCHE, PRATTE, *The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation*, cit., 127 ff.

the interpretation of them made by Canadian judges, the necessity of a *bona fide* claim has to be considered and weighed together *with* the other criteria. The existence of a *bona fide* claim by itself would not be enough to obtain an order of disclosure[286].

There may be more than one reason why this doctrine is now more often applied in Canada than it was some years ago. In particular, the internet environment frequently offers the ideal situation in which a Norwich order can be sought: torts committed by secret defendants whose names are known by third parties (ISPs). The *BMG* case was in this sense paradigmatic: it originated as a "John Doe" case, but it was solved by applying the Norwich standard. This led an author to fear that the Norwich standard would be the only standard applied in all the pre-action discoveries[287].

As we will see, *BMG* considered the privacy of John Does. Until this suit, *Norwich* orders had always dealt with confidentiality. While confidentiality arises from an implicit or explicit agreement between two parties, privacy more simply relates to "intrinsic sensitivity" of certain matters[288]. Before *BMG* one could not advance privacy rights as a defence, since the request did not concern her personal realm, but someone else's one. BMG is also important given that it is the first case applying *Norwich* after the implementation of PIPEDA[289].

c) Irwin Toy

George Irwin was the president of a corporation (Irwin Toy Ltd) who asked for a motion under Ontario Civil Procedure Rules to require an ISP to identify the sender of an e-mail, which had a defamatory content and was directed to more than 70 employees of Irwin Toy. The plaintiff was aware of the e-mail address and could therefore trace the ISP of the sender, but not the sender herself. Although requested by Irwin, the ISP would not disclose the identity of the sender without an order by a court.

[286] LAROCHE, PRATTE, *The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation*, cit., 129.
[287] YIU, 43-44.
[288] For a critical approach to how confidentiality, privacy and data protection have been mixed in the last years see WILKINSON, *Battleground between new and old orders*, cit., 252 ff.
[289] YIU, 63.

The motion was promoted under Rules 30.10 and 31.10[290] against "John Doe", seeking damages for defamation and breach of confidence. The e-mail was indeed defamatory and attached to it there were two files, which were privately and confidentially related to the company and had been wrongfully removed from the corporate computer system. Thanks to a communications and internet consulting firm, Irwin was able to obtain the internet alias of the sender. Later on the plaintiff found out also the IP address, referred to a subscriber of the ISP iPrimus Canada. The ISP confirmed that the IP referred to one of its subscribers and that the electronic records would be preserved. Nevertheless the ISP denied its collaboration for the identification of the wrongdoer unless there was an application of a court order.

The ISP was then notified of the motion proposed by Irwin and closed the account of the customer in question. Despite the knowledge that the ISP would collaborate, Wilkins J. decided to analyze and comment on this form of motion, aware of the fact that probably this type of request would become more frequent in the future[291].

---

[290] Ontario Rules of Civil Procedure, R.R.O. 1990 – *Production From Non-Parties With Leave - Order for Inspection - 30.10* (1) The court may, on motion by a party, order production for inspection of a document that is in the possession, control or power of a person not a party and is not privileged where the court is satisfied that, (a)the document is relevant to a material issue in the action; and (b) it would be unfair to require the moving party to proceed to trial without having discovery of the document. *Notice of Motion* - (2)A motion for an order under subrule (1) shall be made on notice, (a) to every other party; and (b) to the person not a party, served personally or by an alternative to personal service under rule 16.03. *Court may Inspect Document* - (3) Where privilege is claimed for a document referred to in subrule (1), or where the court is uncertain of the relevance of or necessity for discovery of the document, the court may inspect the document to determine the issue. - *Preparation of Certified Copy* - (4) The court may give directions respecting the preparation of a certified copy of a document referred to in subrule (1) and the certified copy may be used for all purposes in place of the original.
Discovery Of Non-Parties With Leave – General - 31.10 (1) The court may grant leave, on such terms respecting costs and other matters as are just, to examine for discovery any person who there is reason to believe has information relevant to a material issue in the action, other than an expert engaged by or on behalf of a party in preparation for contemplated or pending litigation. *Test for Granting Leave* - (2) An order under subrule (1) shall not be made unless the court is satisfied that, (a) the moving party has been unable to obtain the information from other persons whom the moving party is entitled to examine for discovery, or from the person the party seeks to examine; (b) it would be unfair to require the moving party to proceed to trial without having the opportunity of examining the person; and (c) the examination will not, (i) unduly delay the commencement of the trial of the action, (ii) entail unreasonable expense for other parties, or (iii) result in unfairness to the person the moving party seeks to examine. *Costs Consequences for Examining Party* - (3)A party who examines a person orally under this rule shall serve every party who attended or was represented on the examination with the transcript free of charge, unless the court orders otherwise. (4) The examining party is not entitled to recover the costs of the examination from another party unless the court expressly orders otherwise. *Limitation on Use at Trial* - (5) The evidence of a person examined under this rule may not be read into evidence at trial under subrule 31.11 (1).

[291] *Irwin Toy*, paras. 1-9.

First of all, Wilkins J. acknowledged that it is mutually understood that using an alias or a pseudonym on the web means that the identity, to some degree, will remain concealed. This is particularly true when providers inform users that they will safeguard their privacy or conceal their identities. So "[g]enerally speaking, it is understood that a person's internet protocol address will not be disclosed"[292]. In exchange for these policies, sometimes ISPs ask their customers not to send defamatory messages. This approach to confidentiality has, according to Wilkins J., a significant safety value and "should be perceived as being good public policy"[293].

In *Irwin Toy* the claimant had demonstrated on a *prima face* basis that the e-mail content was capable of being defamatory and that the files attached to the e-mail were private and confidential, illicitly removed from the company's computer system. The Court stated that usually under Rule 31.10 the moving party has to satisfy the court that they have been unable to obtain the information from other persons whom she is entitled to examine for discovery. In the judge's words, it was difficult to imagine another way for the plaintiff to identify the Doe than disclosure from the ISP.

The same rule further contemplates imposing on the claimant the burden to demonstrate that there is reason to believe that the person to be examined has information relevant to a material issue in the action. Wilkins J. wrote that the true identity and address could probably always be something of such importance so as to require its disclosure for a defendant. At the same time the Judge recognized that the disclosure should never be automatic, otherwise it could affect the benefits of anonymity on the internet[294].

Since in the particular case the moving party had demonstrated that it has a *prima facie* case and in the judge's opinion it would have been unjust to require the plaintiff to commence a suit only to obtain the real tortfeasor's identity, the Court granted the order with Irwin bearing the costs for the disclosure.

[292] *Irwin Toy*, par. 10.
[293] *Irwin Toy*, par. 11.
[294] *Irwin Toy*, paras. 16-17.

d) CCH

CCH was a case, *inter alia*, where the Supreme Court of Canada ruled on secondary copyright infringement[295]. The appellant – CCH – is a publishing company that provides services for professionals in the area of law. The Law Society of Upper Canada maintains and runs a library in Toronto, with one of the largest collections of legal material in Canada. The library provides a "request-based photocopy" service for Law Society members, the judiciary and other authorized people. Through this photocopy service legal materials were reproduced by the library staff and delivered directly or via mail. In 1993, CCH commenced an action for copyright infringement against the Law Society, for the latter was reproducing a copy of each type of CCH's legal publications. The publishers also tried to obtain a permanent injunction prohibiting the Society from reproducing various works that they had published. The Law Society denied liability and instead counterclaimed for a declaration "that copyright is not infringed when a single copy of a reported decision, case summary, statute, regulation or a limited selection of text from a treatise is made […] for the purpose of research"[296].

The Court of first instance allowed CCH's action in part, holding that the Law Society had infringed copyright in certain works and dismissed the Law Society's counterclaim. Gibson J. however ruled that a great deal of the work was not original. The Federal Court of Appeal allowed the publishers' appeal in part, stating that the works were all original and therefore covered by copyright, though it did hold that much of the reproduction of the work was protected by the concept of fair dealing. It dismissed the Law Society's cross appeal.

[295] I will analyze only the decision of the Supreme Court. Despite secondary infringement is not the core interest of my work, in this decision the Supreme Court gave a number of very interesting definitions and the case is considered a leading one. See, especially for the part of the decision regarding originality W.L. HAYHURST, *The Canadian Supreme Court On Copyright*: CCH Canadian Ltd. v Law Society Of Upper Canada, 41 Can. Bus. L.J. 134 (2004); P. ESMAIL, CCH Canadian Ltd v. Law Society of Upper Canada: *Case Comment on a Landmark Copyright Case*, 10 Appeal 13 (2005). See also T. SCASSA, *Recalibrating Copyright Law? A Comment on the Supreme Court of Canada's Decision in* CCH Canadian Ltd. v. Law Society of Upper Canada, 3 CJLT 89 (2004). GERVAIS, *Canadian Copyright Law Post-CCH*, cit. For lower courts decisions' comments: D.S. MARSHALL, *First Impressions of a Troubling Case: Some Comments on* CCH Canadian Limited v. The Law Society Of Upper Canada, 25 Canadian Law Libraries 19 (2000); A. DRASSINOWER, *CCH Canadian Limited V. The Law Society Of Upper Canada: A Primer*, 28 Canadian Law Libraries 201 (2003).
[296] See *CCH*, summary.q

The case reached the Supreme Court and McLachlin C.J. delivered the judgment of the Court. She questioned whether the Law Society had breached copyright either by providing the custom photocopy service in which the publisher's works were reproduced and sent to patrons upon request or by maintaining the self-service photocopiers and copies of the works in the Library. In Justice McLachlin's view in order to answer these questions the Court should have addressed the following:

1. "[Were] the publishers' materials "original works" protected by copyright?

2. Did the Great Library authorize copyright infringement by maintaining self-service photocopiers and copies of the publishers' works for its patrons' use?

3. Were the Law Society's dealings with the publishers' works "fair dealing[s]" under s. 29 of the Copyright Act […]?

4. Did Canada Law Book consent to have its works reproduced by the Great Library?"[297].

CCH had also filed a cross-appeal in which they claimed that the Law Society infringed their works also by faxing and selling copies of the copyrighted works through its custom photocopy service. Furthermore CCH contended that Great Library did not qualify for library exemption under the Copyright Act. In this case McLachlin C.J. wrote that the Court should have addressed these other questions:

A. "Did the Law Society's fax transmissions of the publishers' works constitute communications "to the public" within s. 3(1)(*f*) of the *Copyright Act* so as to constitute copyright infringement?"

B. Did the Law Society infringe copyright by selling copies of the publishers' works contrary to s. 27(2) of the *Copyright Act*?

C. Does the Law Society qualify for an exemption as a "library, archive or museum" under ss. 2 and 30.2(1) of the *Copyright Act*?

D. To the extent that the Law Society has been found to infringe any one or more of the publishers' copyrighted works, are the publishers entitled to a permanent injunction under s. 34(1) of the *Copyright Act*?"[298]

In analyzing point n. 1, McLachlin C.J. held that for a work to be "original" within the meaning of the Copyright Act this must be more than a copy of another

[297] *CCH*, 347.
[298] *CCH*, 347-348.

work, but at the same time it does not need to be creative, in the sense of being novel or unique. To ask for a minimum degree of creativity avoids the author being overcompensated for the work made and helps in letting enough space for the public domain. To require "originality" would be a too high standard: novelty and non-obviousness are concept more properly related to patents[299]. So, to be protected by copyright, a work shall be "an exercise of skill and judgment". Skill is meant as the use of knowledge, aptitude or practiced ability in producing the work. Judgment is meant as the use of one's capacity for discernment or ability to form an opinion or evaluation. This implies that there has to be more than a mere mechanical exercise[300]. Applying this standard, the Supreme Court found that the works of CCH were all protected by the Copyright Act[301].

Going to question n. 2, the Court investigated whether the Great Library had authorized copyright infringement by maintaining the self-service photocopy machines. Under section 27(1) of the Copyright Act it is an infringement for anyone to do anything that would be allowed only to the owner, including authorizing the exercise of her rights. It does not constitute copyright infringement to authorize a person to do something that would not constitute copyright infringement. The main point here was to understand what it is meant for "authorize". According to McLachilin C.J. this word has to be interpreted in a strict way, in its "strongest dictionary meaning, namely, '[g]ive approval to; sanction, permit; favour, encourage'"[302]. It nevertheless depends on the circumstances of each case and could also be inferred from facts, like indifference. But in the Judge's view this did not mean that merely authorizing the use of equipment that could be used to infringe copyright would mean infringing copyright. Courts should presume that in authorizing an activity, a person does so only in so far as it is in respect of the law[303]. This presumption could be overreached by showing that there is a certain relation or degree of control between the authorized and the infringer.

[299] *CCH*, 356.
[300] *CCH*, 352.
[301] See *CCH*, 358-360.
[302] *CCH*, 361.
[303] Citing *Muzak Corp. v. Composers, Authors and Publishers Association of Canada, Ltd*., [1953] 2 S.C.R. 182, 193.

In reversing what the Court of Appeal had held, the Supreme Court stated that the behavior of the Great Library was not an authorization of breach of copyright. The Library had put a notice indicating that it was not responsible for infringing copies made by the users: holding the Library guilty for this reason would have meant to shift the balance in copyright too much in favor of the copyright owner in spite of the good of society. Even if the users had infringed copyright, the Law Society lacked sufficient control over the users to conclude that it approved the alleged infringement. Between the Law Society and the Great Library patrons there is no master-servant or employer-employee relationship so that there could be an exercise of control. Given these premises, McLachlin C.J. concluded that there had been no authorization by the Society[304].

Along with the just mentioned explanations that the Court gave and that are very important for the application of the Copyright Act, this judgment is mostly famous for having somehow modified the concept of fair dealing. Although often mentioned together with US fair use, the two doctrines have quite a different approach[305]. In fact, fair dealing is worded in a rigid way and contains exceptions only for research or private study (section 29 of the Copyright Act), criticism or review (section 29.1) and news reporting (section 29.2)[306]. This wording is probably the main difference with US fair use, which is open-ended and based on a non-exclusive list of factors[307].

Basically, fair dealing regulates the cases in which a person can use a copyrighted work without asking for permission to the right holder, i.e. as long as

[304] *CCH*, 362-364. Notably the Court explicitly chose not to follow a decision of the Australian High Court that held the exact opposite for the case of photocopiers.
[305] For a comparison of the two, see JUDGE, GERVAIS, *Intellectual Property: The Law in Canada*, cit., 217 ff and GERVAIS, *Canadian Copyright Law Post-CCH*, cit., 157 ff.
[306] *Exceptions – Fair Dealing – Research or private study*: 29. Fair dealing for the purpose of research or private study does not infringe copyright. – *Criticism or review*: 29.1 Fair dealing for the purpose of criticism or review does not infringe copyright if the following are mentioned: (*a*) the source; and (*b*) if given in the source, the name of the (i) author, in the case of a work, (ii) performer, in the case of a performer's performance, (iii) maker, in the case of a sound recording, or (iv) broadcaster, in the case of a communication signal. – *News reporting:* 29.2 Fair dealing for the purpose of news reporting does not infringe copyright if the following are mentioned:(*a*) the source; and (*b*) if given in the source, the name of the (i) author, in the case of a work, (ii) performer, in the case of a performer's performance, (iii) maker, in the case of a sound recording, or (iv) broadcaster, in the case of a communication signal".
[307] C.J. CRAIG, *The Changing Face of Fair Dealing in Canadian Copyright Law: A Proposal for Legislative Reform*, in M. GEIST (ed.), *In The Public Interest: The Future of Canadian Copyright Law*, Toronto, 2005, 440.

that use does not interfere with the copyright holder's rights[308]. Fair dealing provisions do not provide a general defense for a dealing that can be considered "fair", for the fairness of a particular use is relevant only if it was carried out for one of the purposes listed under section 29[309]. When it is not covered by the list in the section, the person has to give sufficient acknowledgment of the source of the copied work. So, there are three requirements: first, the dealing has to be one of the listed; second, it has to be fair; third, sufficient acknowledgment must be given where required by the Act[310].

Several elements have been used to determine whether one is dealing fairly or not, such as the purpose and character of the dealing, the nature of the source work, the effect of the dealing on the potential market for the source work, and so on[311]. As said, fair dealing has always been seen as a rigid doctrine, implying the application of mechanical rules[312]. But in *CCH* both the Federal Court of Appeal and the Supreme Court rejected the classical strict construction of the doctrine and opened a sort of new path for the application of this exemption[313]. The approach taken has broadened the scope of this exception "dramatically"[314]. The "new" approach is closer to the USA one for fair use. Nevertheless, Canadian courts have more flexibility, since they do not have to apply all criteria in each case, some of the criteria (namely numbers 1 and 6) are defined in a more open way than the corresponding US criteria[315]. It has been said that *CCH* transformed fair dealing "from a limited exception to an integral part of the copyright system; from a controversial privilege to a recognized right; from an anomaly in an owner-oriented

[308] HANDA, *Copyright Law in Canada*, cit., 288.
[309] CRAIG, *The Changing Face of Fair Dealing in Canadian Copyright Law*, cit., 439.
[310] HANDA, *Copyright Law in Canada*, Markham, cit., 288.
[311] VAVER, *Copyright Law*, cit., 191; see also MCKEOWN, *Fox on Canadian Law of Copyright and Industrial Designs*, cit., 549 ff.
One of the main reform of Copyright Law which was made through the 1997 Act (An Act to amend the Copyright Act, S.C. 1997, c. 24), enacted a set of exceptions for non-profit libraries, archives, and museums (LAMs).
[312] CRAIG, *The Changing Face of Fair Dealing in Canadian Copyright Law*, cit., 443.
[313] CRAIG, *The Changing Face of Fair Dealing in Canadian Copyright Law*, cit., 438.
[314] ESMAIL, CCH Canadian Ltd v. Law Society of Upper Canada: *Case Comment on a Landmark Copyright Case*, cit., 19.
[315] GERVAIS, *Canadian Copyright Law Post-CCH*, cit., 159; CRAIG, *The Changing Face of Fair Dealing in Canadian Copyright Law*, cit., 448. For a deep comparison between the Canadian fair dealing and the USA fair use see G. D'AGOSTINO, *Healing Fair Dealing? A Comparative Copyright Analysis of Canada's Fair Dealing to U.K. Fair Dealing and U.S. Fair Use*, 53 McGill L. J. 309 (2008).

system to an instantiation of the public-owner balance"[316]. In *CCH* the court went as far as to define fair dealing as a *user right*[317].

Going back to the facts of the case, the question in *CCH* was whether one of the services supplied by the Great Library could fall in the fair dealing provision under section 29 for research or private study. The service consisted in photocopying and sending legal materials upon specific request from a person. First of all, the court recognized that fair dealing is a user's right. This means that in order to maintain the proper balance between the rights of the copyright owner and users' interest, this exception has not to be interpreted too narrowly. A library can always try to prove that its dealing were fair under section 29. In case it was unable to qualify for section 29, a library would need to turn to section 30.2, related to library exemption[318].

For the purposes of section 29, a defendant must prove that the dealing was for the purpose of either research or private study and, in addition, that it was fair. The meaning of the word "research" has to be intended in a broad sense and it has not to be limited to non-commercial activities or private ones. In these terms, lawyers research for the advice of clients or for arguing cases remains research within the meaning of section 29[319]. For what the meaning of "fair" is concerned, the Act does not define it and judges have always recognized that it is not possible to define it[320]. Referring to case law, the Court of Appeal in *CCH* listed a number of factors that

[316] CRAIG, *The Changing Face of Fair Dealing in Canadian Copyright Law*, cit., 461.
[317] *CCH*, 365.
[318] *Research or private study* – 30.2 (1) It is not an infringement of copyright for a library, archive or museum or a person acting under its authority to do anything on behalf of any person that the person may do personally under section 29 or 29.1. *Copies of articles for research, etc.* – (2) It is not an infringement of copyright for a library, archive or museum or a person acting under the authority of a library, archive or museum to make, by reprographic reproduction, for any person requesting to use the copy for research or private study, a copy of a work that is, or that is contained in, an article published in (*a*) a scholarly, scientific or technical periodical; or (*b*) a newspaper or periodical, other than a scholarly, scientific or technical periodical, if the newspaper or periodical was published more than one year before the copy is made. *Restriction* – (3) Paragraph (2)(*b*) does not apply in respect of a work of fiction or poetry or a dramatic or musical work. *Conditions* – (4) A library, archive or museum may make a copy under subsection (2) only on condition that (*a*) the person for whom the copy will be made has satisfied the library, archive or museum that the person will not use the copy for a purpose other than research or private study; and (*b*) the person is provided with a single copy of the work. *Patrons of other libraries, etc.* – (5) A library, archive or museum or a person acting under the authority of a library, archive or museum may do, on behalf of a person who is a patron of another library, archive or museum, anything under subsection (1) or (2) in relation to printed matter that it is authorized by this section to do on behalf of a person who is one of its patrons, but the copy given to the patron must not be in digital form.
[319] *CCH*, 365.
[320] Cf. *Hubbard v. Vosper*, [1972] 2 Q.B. 84 , 94.

could be considered in order to address the fairness of a dealing. The factors, taking into consideration also the US fair use doctrine, are the following:

1) the purpose of the dealing: as already mentioned, for a purpose of dealing to be fair it needs to be one of those listed in sections 29, 29.1 and 29.2 of the Copyright Act, which the Court stated should not be interpreted in a restrictive way[321];

2) the character of the dealing: in judges' opinion, in assessing the character of a dealing, courts should examine the real context, for example giving relevance to the customs or practices within a particular industry[322];

3) the amount of the dealing: this should be considered together with the importance of the work allegedly infringed. In case the amount taken from a work was really small, the court should not even consider the issue of fair dealing, because the action does not constitute copyright infringement. At the same time, the use of the whole work does not *per se* constitute an infringement, because one can fairly deal also with an entire work[323];

4) alternatives to the dealing: in case an alternative non-copyrighted version of the same work was available, this should be considered by the court. This would also help in determining whether the dealing was necessary to reach defendant's purpose or not;

5) the nature of the work: judges should consider whether the work has yet been published or not and, in the latter case, whether the work was obtained by the defendant confidentially or not;

6) the effect of the dealing on the work: in case the reproduced work is a competitor of the original one, this could suggest that the dealing is not fair. Nevertheless this factor should not be considered as the only one or the most important one for the decision of a case[324].

With regard to the dealing in the Great Library, the Law Society showed that the photocopy service was provided for the purpose of research, review and private study. Furthermore the Society did not profit from this service. The fact that those

[321] *CCH*, 366.
[322] *CCH*, 367.
[323] The Court gives an example taken from VAVER, *Copyright Law*, cit., 191: a critic may need to use an entire picture to give her opinion on it.
[324] *CCH*, 368-369.

who requested copies had to identify the purpose of their request and that only one copy of each work would be allowed weighed in favour of finding that the dealings were fair. There seemed to be no alternatives for the photocopy service: researchers are not allowed to borrow materials from the library and the idea of note-taking in the Library seemed unreasonable to the Court. Finally, there had been no evidence that the service provided by the Library could affect the market for the publishers' works. As a result, the court found that the Law Society's dealing with the works was fair[325].

As mentioned above, CCH cross-appealed, submitting that the Law Society had infringed copyright also by faxing and selling copies of the works, because these transmissions were communication to the public by telecommunication. The Supreme Court agreed with the lower ones in considering that this kind of communication was not public, since they emanate from a single point and are sent to another single point[326].

The Court then analyzed the possibility of a secondary infringement of copyright. This would have needed the existence of three different elements: a primary infringement; a second infringer who knew or should have known that she was dealing with a product of infringement; the sale of the illegal copy. Since the main appeal ended saying that there had been no infringement, without a primary infringement there could not be a secondary one. Again, in the main appeal the Law Society's service qualified as a fair dealing. Nonetheless, the Great Library would have qualified for the "library" exemption, since it is not conducted for profit, it is not administered or controlled by a body established for profit and it is open to researchers[327]. The cross appeal was therefore dismissed.

e) Tariff 22

Even if not cited in the BMG cases, it is worth recalling here also the seminal decision denominated "*Tariff 22*". This case is extremely important for the issue of ISPs' liability in the Canadian context. In fact, unlike the USA and Europe, Canada has not implemented a coherent system of legislative norms to regulate this subject

[325] *CCH*, 372-375 *sic passim*.
[326] *CCH*, 376.
[327] *CCH*, 377-378.

as yet. As demonstrated in recapping the US cases, ISPs' liability played an important role in shaping the track which led to John Doe cases.

SOCAN – the Society of Composers, Authors and Music Publishers of Canada – is the Canadian copyright collective society for the performing rights of creators and publishers of music[328]. In 1995 SOCAN proposed "Tariff 22", the first tariff on royalties payable with respect to music transmitted on the Internet[329]. The tariff was set with the Copyright Board[330] that determined also which activities of internet entities infringed copyright and made them potentially liable to pay a royalty. The activities that generated the duty to pay a royalty were those included in the definition of "communication" of the Copyright Act[331].

The Board ruled that only certain Internet intermediaries would "communicate" and therefore infringe copyright. According to the Board, "communication" occurs when a work is transmitted from the host server to the computer of the end user. A communication can be considered made "to the public" either when files are openly made available on the internet or when they are communicated to individual members of the public at different times. ISPs acting as mere intermediaries could not be held liable for copyright infringement; the same

[328] See SOCAN's website: http://www.socan.ca/jsp/en/pub/about_socan/what_we_do.jsp. The following synthesis of the case is extracted from the decision of the Federal Court – *Society of Composers, Authors and Music Publishers of Canada (SOCAN) v. Canadian Association of Internet Providers,* [2002] 4 F.C. 3, paras. 22-30 [*Tariff 22 Federal Court*]. The decision of the Copyright Board as well as those from the upper Courts dealt also with the problem of understanding the origin of a communication, in order to decide whether to apply Canadian law to that communication or not. We will not, however, touch this point, since it is not relevant for our research. For a comment of the case: B. SOOKMAN, *Case Comment: Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Service Providers*, 3 Canadian Journal of Law & Technology 149 (2004).

[329] Tariff 22 was filed in relation to the "licence to communicate to the public by telecommunication, in Canada, musical works forming part of SOCAN's repertoire, by a telecommunications service to subscribers by means of one or more computer(s) or other device that is connected to a telecommunications network where the transmission of those works can be accessed by each subscriber independently of any other person having access to the service", see Copyright Board: Statement of Proposed Royalties to be Collected by SOCAN for the Public Performance or the Communication to the Public by Telecommunication, in Canada, of Musical or Dramatico-Musical Works for the Year 1999, C. Gaz. I. 1998. Supplement June 13 at 26, available at : http://www.gazette.gc.ca/archives/p1/1998/1998-06-13/pdf/g1-13224.pdf.

[330] See *Tariff 22* cit.

[331] Copyright Act Section 2.4(1)(b): "Communication to the public by Telecommunication": 2.4(1) For the purposes of communication to the public by telecommunication, […] (*b*) a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public".

could be said for caching providers[332]. SOCAN applied for judicial review to the Federal Court, which granted the application in part[333].

The Federal Court held that in order for an ISP to qualify for the exception of 2.4(1)(*b*) of the Copyright Act, and therefore not be liable, it is required that the intermediary's means of telecommunication be necessary for enabling another person to communicate. "Necessary" signifies that without the intermediary's activity, the other person could not communicate at all[334].

The Federal Court did not completely agree with the Copyright Board. In particular, the Court agreed on the fact of control, accepting that host servers do not control what is exchanged through their networks and that host server operators do not lose their protection just because they provide their normal communication facilities. The Court, on the contrary, did not agree on caching providers. Caching is not, according to the Court, a "necessary" activity. Furthermore, the cache operator is actually communicating by telecommunication and it is not just a passive transmitter of data, given that it chooses which material should be cached[335].

On the meaning of "authorization" of a communication, the Federal Court hold that an approval, consent or claim would be needed and that the authorization could not be inferred merely by the supply of the equipment enabling the communication[336].

The ISPs appealed to the Supreme Court to obtain a review in relation with

---

[332] See *Tariff 22 CB*, paras. 124-125. A cache is a way to temporarily storing files copied from other sources. It is often used by ISPs in order to reduce time and cost of retrieving and transmitting information across the Web, and increase its reliability, see *Entry: Cache*, SOOKMAN, *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions*, cit., 42. As the Supreme Court itself explained, "[w]hen an end user visits a Web site, the packets of data needed to transmit the requested information will come initially from the host server where the files for the site are stored. As the pass through the hands of an Internet Service Providers, a temporary copy may be made and stored on its server. This is a cache copy. If another user wants to visit this page shortly thereafter, using the same Internet Service Provider, the information may be transmitted to the subsequent user either directly from the Web site or from what is kept in the cache copy. The practice of creating "caches" of data speeds up the transmission and lowers the cost"; see *Society of Composers, Authors and Music Publishers of Canada (SOCAN) v. Canadian Association of Internet Providers*, [2004] 2 S.C.R. 427, par. 23 [*Tariff 22 Supreme Court*].

[333] *Society of Composers, Authors and Music Publishers of Canada (SOCAN) v. Canadian Association of Internet Providers,* [2002] 4 F.C. 3 [*Tariff 22 Federal Court*].

[334] *Tariff 22 Federal Court*, par. 132.

[335] *Tariff 22 Federal Court*, paras. 134-142 *sic passim*. On this point there was a dissenting opinion of Sharlow J.A., who concluded that the Copyright Board was right when stated that caching is an activity ancillary to internet communication and therefore caching providers are entitled to the protection of s. 2.4(1)(b). See *Tariff 22 Federal Court*, paras. 196-197.

[336] *Tariff 22 Federal Court*, paras. 149-162 *sic passim.*

the act of caching; SOCAN cross appealed and asked the Court to hold that also host providers could be liable.

The Supreme Court, which delivered its opinion through the words of Binnie J., agreed with the Copyright Board on the meaning of "communication by telecommunication". Specifically, in 1988 amendments to the Copyright Act[337], "telecommunication" was defined as "any transmission of signs, signals, writings, images or sounds or intelligence of any nature by wire, radio, visual, optical or other electromagnetic system". The Board had held that telecommunication occurs when music is transmitted from the host server to the end user: on this point the Supreme Court agreed[338].

As mentioned, despite Canada being a signatory of the WIPO Copyright Treaty, this has not been ratified yet in the pre-Bill C-11 context. Article 8 of the Treaty provides for authors a right to "make available" their works to the public. Given that in Canada copyright law , the only remedies are provided by the Copyright Act itself. Hence, one can demonstrate the infringement of a right only if it is contained in the Act itself, such as the right to "communicate to the public by telecommunication"[339]. The already cited amendment of 1988 specified that the participant in a telecommunication that only provides for "the means of telecommunication" cannot be considered "communicator". This is what it is actually written in Section 2(4)(1)(*b*) and means that intermediaries are not just "immune" to the infringement occurred, but rather that they are not even part of the communication[340]. In the Court's opinion, to qualify for the mentioned section, the means provided by the intermediary can be of a varying nature. What it is really needed is that the ISP "does not itself engage in acts that relate to the content of the communication". Therefore those whose participation is neutral and supply only a "conduit" for communication will fall within Section 2(4)(1)(*b*). This in turn means that the only person who is liable for the communication is the one who makes the work available for the communication, that is the content provider (or final user), as

[337] *An Act to Amend the Copyright Act and to Amend Other Acts in consequence thereof*, R.S.C. 1985, C. 10.
[338] *Tariff 22 Supreme Court*, par. 42.
[339] *Tariff 22 Supreme Court*, paras. 82-83.
[340] *Tariff 22 Supreme Court*, paras. 86 ff. "[T]hose who participate in the retransmission "solely to serve as an intermediary between the signal source and a retransmitter whose services are offered to the general public" should not be unfairly caught by the expanded definition", see specifically par. 88.

the Copyright Board has concluded[341].

In the Court's view this interpretation would be consistent with the WIPO Copyright Treaty, which states "[i]t is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention"[342]. The lack of actual knowledge with respect to the information transmitted and the impracticability of monitoring the huge amount of data moving through the web are essentially the requirements of a "conduit" ISP, which can benefit of the provision of section 2.4(1)(*b*). Nevertheless, if a provider has notice of infringing material posted on its servers and it is asked to remove it, but it does not, then it can be considered liable due to an authorization of communication of copyrighted material[343].

As far as caching was concerned, Binnie J. acknowledged that was "a serendipitous consequence of improvements in Internet technology". It simply helps in accelerating the exchange of data in the Web. Its use is needed to deliver faster and more economic service and should not, for this reason, be thought as something on which liability should be based[344]. The Court took an approach that differed from the one taken by the lower court, for the fear that a too strict interpretation could have a chilling effect on technology[345].

The Supreme Court then analyzed the question of "authorization" and made a comparison with the mentioned CCH case. SOCAN argued that even if ISPs did not themselves infringe copyright, they were nevertheless guilty of "authorizing" users to do so, because intermediaries know of the existence of uploaded infringing material. As seen, in CCH the Court held that a person does not authorize the infringement by allowing the use of equipment which could be used to infringe

[341] *Tariff 22 Supreme Court*, paras. 92 ff. The Court (at par. 96) made a comparison with "[t]he owners of the telephone wires, who are utterly ignorant of the nature of the message intended to be sent, [and therefore] cannot be said within the meaning of the covenant to transmit a message of the purport of which they are ignorant. (*Electric Despatch Co. v. Bell Telephone Co.* (1891), 20 S.C.R. 83 (S.C.C.), at p. 91).

[342] See "Agreed statements concerning Article 8" of the WIPO Copyright Treaty.

[343] *Tariff 22 Supreme Court*, paras. 97-110 *sic passim*.

[344] *Tariff 22 Supreme Court*, paras. 114-115.

[345] In the Supreme Court's word: "[t]his is a high eligibility test which could inhibit development of more efficient means of telecommunication. SOCAN and others representing copyright owners would always be able to argue that whatever the advances in the future, a telecommunication could still have been practicable using the old technology, and that one way or the other the telecommunication would "in all probability" have occurred", *Tariff 22 Supreme Court*, par. 113.

copyright. Judges should presume that allowance is given only accordingly with the law. The contrary can be proved through showing a relationship or degree of control between the authorized and the primary infringer. Hence, as the Board had stated, "[a]n intermediary would have to sanction, approve or countenance more than the mere use of equipment that may be used for infringement"[346]. Anyway, as already said, things can change if the ISP becomes aware of the infringing content[347]. However, this knowledge could still not be sufficient to constitute authorization, and a case-by-case analysis would be the best approach.

Justice LeBel dissented in part. Firstly, he underlined that the Court should have interpreted the Copyright Act in light of the WIPO Treaty, given that Canada signed it[348]. This would have permitted the application of the authors' right to "make available" to the public and would have given importance to the ISPs' role in the communication, which LeBel J. thought was important.

The second concern of the dissenting judge was related to privacy. In his opinion the "Court should adopt an interpretation of s. 3(1)(f) [*of the Copyright Act*] that respects end users' privacy interests, and should eschew an interpretation that would encourage the monitoring or collection of personal data gleaned from internet-related activity within the home"[349]. Justice LeBel thought that locating the communication at the place of the host server would have addressed privacy concern[350]. In fact, since it was the content provider who made the information available to the public, this would create little concern for privacy violations. On the contrary, the test adopted by the Court, given that it looked at the retrieval practices of the individual user, would encourage the monitoring of users' surfing and download. In Justice LeBel's words this information tends to reveal "core

[346] *Tariff 22 CB*, par. 148.
[347] This is the approach introduced by the DMCA § 512(b) and by the art. 13 of the European Directive 2000/31 ("Directive on electronic commerce"). The Court indeed called on the Parliament for an intervention with a statutory "notice and take down" procedure on the shape of Europe and USA. An approach of this kind is now part of Bill-11 pending at the Parliament, see *supra*.
[348] To justify his point of view LeBel J. cited a recent case *R. v. Sharpe*, [2001] 1 S.C.R. 45, par. 175: "the legislature is presumed to respect the values and principles enshrined in international law, both customary and conventional. These constitute a part of the legal context in which legislation is enacted and read. In so far as possible, therefore, interpretations that reflect these values and principles are preferred", see *Tariff 22 Supreme Court*, par. 150.
[349] *Tariff 22 Supreme Court*, par. 153.
[350] Remember that this case had to deal also with the problem of understanding whether a communication was made inside or outside Canada, in order to apply Canadian law and the Tariff 22 itself. This is why Justice LeBel talked about "locating" the communication at the host server level.

biographical information about a person" and the Court should therefore eschew to adopt a solution which may encourage such monitoring[351].

3.3.3 Justice Von Finckenstein's decision in BMG v. Doe

Let us now go back to BMG case, which concluded on the 31st of March 2004, when Justice Von Finckenstein delivered his decision. After summarizing the facts and explaining, through the words of the famous US case of *MGM v. Grokster*[352], how a peer-to-peer file sharing system works, the judge asked himself three questions:

1. "What legal test should th[e] Court apply?
2. Have the plaintiffs met the test?
3. If an order is issued, what should be the scope and terms of such order?"[353].

The Court referred to *Norwich* and *Glaxo Wellcome*, which, as seen, have established that when an applicant seeks pre-action discovery to ascertain the identity of a defendant, she can do this through an equitable bill of discovery. Whereas, Von Finckenstein J. explained that, when an action has been started, even if against a "Doe" defendant, the plaintiff has to rely on the cited Rules 233 and 238.

The cited cases explained which criteria should be applied in order to grant the discovery. In particular, as the federal judge held, the first two threshold requirements are that the appellant has a bona fide claim and that she shares a sort of relationship with the respondent. These requirements are intended to avoid respectively that an action be frivolously brought and that a bill of discovery be issued against a mere witness or disinterested bystander. Furthermore, another basic condition for granting a bill of discovery is that the person from whom the information is sought is the only practical source of information available to the applicant. An example would be a case where the appellant could not even bring an action if the respondent does not make available the information by discovery. As seen, the House of Lord in Norwich took also into account the *public* interests existing for and against the disclosure. In particular, on the one hand a judge should

[351] *Tariff 22 Supreme Court*, par. 154-155.
[352] *Grokster District Court*, 1032-1033.
[353] *BMG I*, par. 8.

evaluate the possibility of an expectation of privacy and on the other hand she should consider (among others) the standpoint of the State in ensuring the effective administration and enforcement of law[354]. Given this preamble, Von Finckenstein J. listed the following five criteria, which in his opinion should have been applied also to motion promoted under Rule 238:

a) "the applicant must establish a prima facie case against the unknown alleged wrongdoer;
b) the person from whom discovery is sought must be in some way involved in the matter under dispute, he must be more than an innocent bystander;
c) the person from whom discovery is sought must be the only practical source of information available to the applicants;
d) the person from whom discovery is sought must be reasonably compensated for his expenses arising out of compliance with the discovery order in addition to his legal costs;
e) the public interests in favour of disclosure must outweigh the legitimate privacy concerns"[355].

For what the motion under Rule 233 was concerned, the Court determined that this rule was not broad enough to cover the requests of the plaintiffs. Indeed, this rule applies to the production of existing documents and in the particular case where documents should have been specifically generated by the ISP, given that they were not already in existence[356]. Once ascertained, the federal judge went back to the five criteria, analyzing each of them.

With regard to criterion a), the Court found three defects:

1) the affidavit was deficient as to content: as pointed out by Bell and Telus responses, Mr Millin's affidavits relied mainly on hearsay. Federal rules of civil procedure make hearsay admissible provided that the grounds for belief are stated[357]. Nevertheless, Mr Millin did not give reason for his beliefs and

[354] *BMG I*, par. 12 (emphasis added).
[355] *BMG I*, paras. 13-14.
[356] *BMG I*, par. 15.
[357] *Content of affidavits* - 81. (1) Affidavits shall be confined to facts within the personal knowledge of the deponent, except on motions in which statements as to the deponent's belief, with the grounds therefor, may be included. - *Affidavits on belief* - (2) Where an affidavit is made on belief, an adverse inference may be drawn from the failure of a party to provide evidence of persons having personal knowledge of material facts. (Federal Court Rules, 1998, SOR/98-106). Note that the first part of this

the source of the information was not stated. Moreover, Mr Millin said he was not able to say whether any of the files allegedly copied by MediaSentry from the alleged infringers' folders were in fact any infringed files of the plaintiffs[358];

2) the judge could not find evidence of connection between the pseudonymous and the IP addresses. Mr Millin's affidavit did not explain or give proof of how the nicknames were linked to the IP addresses identified by his company. Without this evidence and without being able to understand its reliability, "it would [have been] irresponsible for the Court to order the disclosure of the name of the account holder […] and expose this individual to a law suit by the plaintiffs"[359];
3) the plaintiffs had not showed evidence of infringement of copyright. "Copyright law can be invoked by owners only to the extent explicitly set forth in the statute". Ironically, the Court cited the same decision of the Copyright Board cited by CRIA[360], but reached a different conclusion: downloading a song for personal use does not amount to infringement in the light of Section 80(1) of the Copyright Act[361].

   Von Finckenstein J. implicitly agreed with CIPPIC in saying that Does simply put personal copies into their shared directories. This did not amount to authorization of infringement. As earlier explained, citing *CCH*, the judge claimed that he could not see the "difference between placing 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". For an act to constitute "distribution" there should be a positive act, such as sending the copies or advertising their availability. The simple "right to make available" was not part of the Canadian copyright law, given that Canada had not yet implemented WIPO Treaties. Finally, plaintiffs had not demonstrated

Rule has now changed: *Content of affidavits* - 81. (1) Affidavits shall be confined to facts within the personal knowledge of the deponent, except on motions in which statements as to the deponent's belief, with the grounds therefor, may be included (SOR/2009-331, s. 2).

[358] *BMG I*, paras. 16-19.
[359] *BMG I*, par. 20.
[360] *Private Copying 2003-2004*, 20.
[361] *BMG I*, paras. 21-25.

that users were in fact infringing copyright. Direct infringement is the precondition for a secondary infringement to verify[362].

As for criterion b), there was no doubt that ISPs were involved with the alleged infringer, given that the former provided access to the Internet to the latter[363].

Criterion c) regarded the "only practical form of information" requirement. Since Mr Millin's and Ms Yonekura's affidavits did not mention who operated the P2P networks, the Court could not make a determination on this point[364].

Criterion d) provides that the person from whom the discovery is sought shall be compensated for the expenses borne due to compliance with the discovery order, as well as legal costs. From the ISPs' affidavits, the Court drew some conclusions. First of all, the kind of information sought by the plaintiffs was not normally kept by the ISPs. Furthermore, the older the information is, the more difficult would be to collect it and the more unreliable it would be. Given that some time had passed, linking some IP addresses to account holders could have been impossible. Moreover, even if ISPs could find out the name of the account holder, they would never find the actual computer user, especially when the account holder was an institution. Even not taking these problems into account, the process would have been costly for the ISPs and they would have needed to be reimbursed for all the expenses[365].

Finally, Von Finckenstein J. undertook the issue of the public interests in favour and against the disclosure of the data. He stated that "[i]t is unquestionable but that the protection of privacy is of utmost importance to Canadian society"[366]. He then cited the words of Justice Lamer in *R. v. Dyment*: "[g]rounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order" [367]. Then the judge referred to *Irwin Toy*, where Wilkins J. noticed that in the usage of the Internet some degree of confidentiality or of privacy with regard to the IP address of users is considered as being good public policy. The same judge further stated that generally it was

[362] *BMG I*, paras. 26-29.
[363] *BMG I*, par. 30.
[364] *BMG I*, par. 31.
[365] *BMG I*, paras. 32-35.
[366] *BMG I*, par. 36.
[367] *R. v. Dyment*, cit., par. 28.

understood that this kind of data would not be disclosed and that ISPs exchanged this confidentiality obligation with their customers' agreement that they will not transmit defamatory or libelous messages[368].

Justice Von Finckenstein then turned to PIPEDA. Despite recognizing that Parliament, in enacting PIPEDA, had agreed on the need of protecting privacy, this did not mean that privacy could be used to protect a person from the application of liability. In particular, according to the federal judge, PIPEDA does not restrict the ability of a Court to order production of documents related to the identity of that person. Indeed, Section 7(3)(c) allows disclosure without consent of the data subject if "required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records"[369]. Therefore both PIPEDA and the *Norwich/Glaxo Wellcome* test would have permitted the disclosure of the requested data. Indeed, previous cases demonstrated that privacy had never outweighed the interests in obtaining the disclosure[370].

Nevertheless the Court wanted to be sure that the information disclosed would have been reliable. The evidence was gathered some months earlier that the motion was filed and this could make the information difficult to obtain and could decrease its reliability. These problems could lead to the identification of the wrong persons. Therefore the Court stated that "the privacy concerns outweigh[ed] the public interest concerns in favour of disclosure"[371].

Justice Von Finckenstein analyzed then the second question, i.e. whether the plaintiffs had met the test. Following the premises, the judge's conclusion was that the test had not been met. Plaintiffs had neither made out a *prima facie* case, nor had they demonstrated that ISPs were the only practical source of information, nor had they established that the public interest for disclosure was bigger than the privacy concerns, given the old age of the data[372].

---

[368] *Irwin Toy*, paras. 10-11.
[369] PIPEDA - Section 7(3)(c).
[370] Justice Von Finckenstein made reference to *Irwin Toy*; *Ontario First Nations Limited Partnership v. John Doe*, (3 June 2002) (Ont.S.C.J.); *Canadian Blood Services/Société Canadienne du Sang v. John Doe*, (June 17, 2002) (Ont. S.C.J.); *Wa'el Chehab v. John Doe*, (October 3, 2003) (Ont. S.C.J.); *Kibale v. Canada*, [1991] F.C.J. No. 634 (QL) (FC); *Loblaw*.
[371] *BMG I*, paras. 36-42.
[372] *BMG I*, par. 43.

Finally, the federal judge considered the hypothesis in which the disclosure had been granted. In that case certain restrictions would have been necessary in order to protect Does' privacy: first, the name should have been disclosed only for the purposes of the claim and, second, an annex subject to a confidentiality order should have been added to the statement of claim relating each pseudonym to the name and address of the account holder[373].

As a result of his finding, the judge denied the motion.

3.3.4 BMG v. Doe case in front of the Federal Court of Appeal

Only a couple of weeks later than Justice von Finckenstein's order, CRIA appealed his decision[374].

CRIA justified its appeal on the premise that the judge had erred in the application of the legal test. Basically, CRIA repeated the same arguments it had used in proposing its motion. In the recording industry's opinion, the federal judge had mistakenly interpreted Section 80(1). In CRIA's vision, the Does had copied the recording not merely for personal use; rather they had copied them in their shared directories with the aim to distribute and communicate the songs[375]. With regard to the alleged infringement of authorization rights under Sections 18(1) and 27(1), CRIA insisted in stating that file sharing software are "designed to facilitate the reproduction, transmission and distribution of sound recordings", that the defendants "placed the appellants' sound recording in share directories on their computers" and "connected to a peer-to-peer network […] displaying to a vast number of Internet users the contents of the shared directories as being freely available"[376].

The judge should have recognized the existence of a *prima facie* or *bona fide* standard, given that CRIA had demonstrated that the defendants had knowingly copied and distributed appellants' works, sending them out, in this way infringing appellants' distribution rights under Section 27(2)(b). Von Finckenstein J. had erred in holding that the plaintiffs had not demonstrate the link between users'

[373] Furthermore Justice von Finckenstein held that in case of disclosure, the ISPs would have not been required to provide an affidavit and the mere disclosure of the defendants' names and last known address would have been sufficient; see *BMG I*, paras. 44-46.
[374] *CRIA's notice of appeal* is available at http://www.cippic.ca/documents/file-sharing-lawsuits/criaappealnotice.pdf [*CRIA's appeal*].
[375] *CRIA's appeal*, 6.
[376] *CRIA's appeal*, 6-7.

pseudonymous and the IP addresses and that ISPs were not the only practical source for the information sought[377].

Furthermore the judge had erred in saying that it was common ground that subscribers had an expectation that their identity would be kept private and confidential and that the data were not reliable due to their obsolescence.

Finally, the judge erred in holding that Rule 233 presupposes the existence of the requested documents, since computer data were already available on the computer systems of the ISPs[378].

In May 2005, the Federal Court of Appeal delivered its decision, which went in the same direction of Justice Von Finckenstein's as regards the evidence, though not completely in accordance with his view as regards s. 80.

In the opening words of Sexton J.A., the "case illustrate[d] the tension existing between the privacy rights of those who use the Internet and those whose rights may be infringed or abused by anonymous Internet users"[379]. Sexton J.A. engaged in an interesting reasoning where he expressed his concerns regarding privacy. He acknowledged that current unwarranted intrusions do not have precedents. This intrusion puts individuals at great personal risk and subjects their views and belief to indefensible scrutiny. This is why privacy advocates ask for a strong *prima facie* case against the individuals whose data were going to be revealed[380].

After re-telling the facts, the argumentation of each party and the decision taken by the lower court, the Court of Appeal started its analysis. Addressing the issue of the applicability of Rule 233, Sexton J.A. agreed with Von Finckenstein J. in saying that the information sought did not currently exist and that it needed to be produced. Therefore the mentioned Rule could not be applied[381].

With regard to Rule 81, and the deficiencies in the plaintiffs' materials, the Court wrote that much of the crucial evidence submitted by CRIA was indeed hearsay and no ground was provided for accepting that hearsay. This inaccuracy of the evidence could have led to the wrong people, creating the risk of invading the

[377] *CRIA's appeal*, 7-8.
[378] *CRIA's appeal*, 8.
[379] *BMG II*, par. 1.
[380] *BMG II*, par. 4.
[381] *BMG II*, paras. 17-19.

privacy of innocent account holders, who could be named as defendants. Justice Sexton held that the appeal should have been dismissed for this reason alone[382].

According to Sexton J.A., in spite of the arguments of the ISPs, Rule 238 was applicable in the case. Rule 238(2) provides that notice of the motion must be served "on the other parties". Since the other parties are not known (the Does), the ISPs argued that the service was not possible and therefore Rule 238 could not provide a procedure to discover the identities. Rule 238(1) provides that "[a] party to an action may bring a motion for leave to examine for discovery any person not a party to the action […] who might have information on an issue in the action". As argued by the plaintiffs, the main issue on the motion was the identity of the alleged infringers and in the Court of Appeal's reasoning this was an issue in the action and that Rule 238 was broad enough to cover this case. In particular, Justice Sexton admitted that examinations for discovery of third parties were not routinely ordered and that this should not become common, but that they are nevertheless applicable. He went further and stated that orders under Rule 238 would be necessary when a plaintiff would be frustrated in enforcing her rights, because she is unaware of the identity of the alleged wrongdoers. To sustain his argument, the judge compared Rule 30.10 and 31.10 of Ontario Rules of Civil Procedure to Rule 238. In *Irwin Toy* the Ontario Superior Court of Justice held that those rules could be used to compel production from ISPs of the identity of senders of e-mails. Similarly, in *Loblaw* the New Brunswick Court of Queen's Bench applied a comparable rule to compel production of the identity of an individual who had sent an e-mail containing confidential information that could have given rise to an action for damages[383].

[382] *BMG II*, paras. 20-21.

[383] New Brunswick Rule of Court, N.B. Reg. 82-73 - *32.12 Discovery before Commencement of Proceeding* - (1) On such terms as may be just, the court may grant leave to any person to examine for discovery, before commencement of proceedings, any other person who may have information identifying an intended defendant. (2) An application under paragraph (1) shall be made by preliminary motion on notice to the person sought to be examined and shall show that (a) the applicant has a prima facie case for relief against the intended defendant, (b) the applicant, having made reasonable inquiries, has been unable to identify the intended defendant, and (c) the applicant has reason to believe that the person to be examined has knowledge of facts, or has in his possession, custody or control documents or things identifying the intended defendant. Loblaw is a decision which arose from following but very similar case to *Irwin Toy*. The case was decided by the New Brunswick Court of Queen's Bench. The plaintiff is Canada's largest food distributor. Someone had obtained information on the company's payroll regarding a number of senior employees of Loblaw. This information was then included in an e-mail sent to a large number of the applicant's employees. Since the spread of these data could give rise to an action for damages against the person who sent the e-

Turning to the applicability of a bill of discovery, the Court cited *Glaxo Wellcome* again. In that decision the Court stated that this remedy permits a court, acting in equity, "to order discovery of a person against whom the applicant for the bill of discovery has no cause of action and who is not a party to contemplated litigation […], who is in some way connected to or involved in the misconduct"[384]. Justice Sexton agreed with the Trial Division in holding that the same criteria used for granting a bill of discovery should have been applied also under Rule 238, given that the same issue was at stake in both procedures. However, Sexton J.A. disagreed with regard to the description of the first aspect of the test to be applied. While Justice Von Finckenstein had said that the plaintiff should provide evidence of a *prima facie* case, the appellate Court stated that the proper test was whether the applicant had a *bona fide* claim against the proposed defendant. Sexton J.A. referred again to *Glaxo Wellcome*. In *Glaxo Wellcome* Stone J.A. held that, despite a different application made by some other courts, the *Norwich* approach did not require the plaintiffs to show the she would likely succeed at trial. Rather, the plaintiff should only show to have a *bona fide* belief that the persons whose names are sought had infringed her right[385]. Justice Sexton recognized that it was impossible for the plaintiffs to prove a *prima facie* case, given that they did not even know the identity of the alleged infringers, and therefore they did not know their behavior. For these reasons the Court of Appeal suggested that the proper standard required a *bona fide* claim[386].

As for the other criteria relating to the equitable bill of discovery, the appellate Court agreed with Justice Von Finckenstein. CRIA had not demonstrated that the ISPs were the only source of information. Furthermore the Court held that in case of disclosure consideration should have been given to the costs which the ISPs had suffered[387].

---

mail, Loblaw tried to identify the sender. The claimant could only ascertain that the e-mail account was a Yahoo! one and found out the ISP to which the IP address was linked. Therefore Loblaw cited the ISP (Aliant Telecom) to obtain discovery of the identity of the e-mail sender, in accordance with New Brunswick Rules of Court above quoted. Applying the case law and referring also to *Norwich* the Court held that Loblaw had met all the requirements and granted the application. See *BMG II*, paras. 23-27.

[384] *Glaxo*, par. 20.

[385] *Glaxo*, par. 44.

[386] *BMG II*, paras. 28-34.

[387] *BMG II*, par. 35.

The Court of Appeal then addressed the delicate question of privacy. Sexton J.A. agreed with the lower court in saying that in order to permit the disclosure, public interest should have outweighed legitimate privacy concerns. Under PIPEDA, ISPs are not entitled to voluntary disclose personal information of their customers. Nevertheless, as seen, they can be compelled to reveal this information pursuant to a court order. Moreover, when an organization receives a request for the release of personal information, it "shall retain the information for as long as is necessary to allow the individual to exhaust any recourse" under the Act[388]. In order to protect people's privacy, PIPEDA provides that the disclosure of personal information handled by organization can be done only in certain circumstances under subsection 7(3). Indeed, one of the purposes of PIPEDA was "to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances"[389]. The Court of Appeal held that even if modern technology has had great benefits for society, this should not mean that technology permits to "obliterate those personal *property* rights which society had deemed important". It seemed to Justice Sexton that, although privacy concerns have to be considered, they must surrender to public concerns related to the infringement of intellectual property right, where this "*infringement threatens to erode those rights*". Therefore, when plaintiffs show that they have a bona fide claim that unknown individuals are infringing their copyrights, they have a *right* to obtain the identity of those persons for the purpose of starting a lawsuit[390]. Nevertheless, this disclosure has to be made with caution to be sure that the alleged infringers' privacy rights are invaded as least as possible.

Going back to the actual case, the Court considered the question of the lengthy delay between the request for the identities made by CRIA and the time the recording industry had collected the information. The possible inaccuracy of the information, linked to the dynamicity of the IP addresses, could have led to the

[388] PIPEDA – *Retention of information* – 8(8).
[389] PIPEDA – *Purpose* – 3.
[390] *BMG II*, paras. 41-42 (emphasis added).

infringement of the privacy rights of innocent persons, who could have then be sued by CRIA without justification. Avoiding this delay is important, since failure to take such care could justify a court in refusing to make a disclosure order. Furthermore, as CIPPIC had pointed out, Justice Sexton stressed that plaintiffs should be careful not to extract defendants' private information not related to the infringement of copyright. This information could indeed be highly confidential and an intrusion in this data could result in a breach of PIPEDA by the ISPs, with liability consequences. Finally, the Court held that if the disclosure had been granted, specific direction should have been given as to the type of information disclosed and the manner in which this information could be used[391].

In the end, the Court of Appeal turned to the question of copyright infringement. After stating that the lower court should have not made any conclusion about the infringement in the very early steps of the lawsuit, Justice Sexton addressed some points. According to him, the lower court had not correctly applied subsection 80(1) of the Copyright Act. Indeed, it appeared that Justice von Finckenstein had not considered whether all the requirements for the application of the exemption in relation to personal use were met. The Trial Division Judge relied upon *CCH*, but he did not consider whether copying the songs into a shared directory could constitute authorization because it invited and permitted other users to have access to them and copy them. The Trial Division stated that "distribution" meant a "positive act" by the owner of the shared folder. But to the mind of Sexton J.A., this interpretation of "distribution" was not so clear in the legislation. Finally, Von Finckenstein J. had stated that there could not be a secondary infringement, because users were not aware of the copying of someone else. The appellate court dissented, for indirect infringement could exist also when the user "should have known" that there was infringement. Justice Sexton concluded saying that such findings were made too early in the case[392].

"In the result, the appeal [was] dismissed without prejudice to the plaintiffs' right to commence a further application for disclosure of the identity of the "users" taking into account these reasons". Richard C.J. and Noël J. A. agreed[393].

[391] For example a user could be identified only by initials; see *BMG II*, paras. 35-45.
[392] *BMG II*, paras. 46-54.
[393] *BMG II*, par. 55.

3.3.5 Latest developments in the battle against file sharers

At the end of August 2011, the Federal Court released its decision on *Voltages Pictures LLC v. Jane Doe and John Doe*[394]. Voltages Pictures is a production company, which is the owner of the copyright on the movie "The Hurt Locker"[395]. After launching actions against many users in USA, the company moved to Canada in order to fight against the alleged illegal sharing of the mentioned movie[396]. Exactly in the same way CRIA had done for music, Voltage Pictures had detected IP numbers of users allegedly downloading the movie. Again, as in BMG cases, the plaintiff was not able to obtain users' names without the help of the ISPs. Therefore, the claimant asked for a written examination for discovery of the ISPs in order to obtain the names and addresses of the users corresponding to the IP numbers, to eventually sue them[397].

Insofar as can be gleaned from reading the decision, the Federal Court, relying on an affidavit, accepted the claim that the defendants downloaded and distributed the movie through P2P networks, relied on an affidavit[398]. The Court failed to follow the more stringent test applied by the Trial Division in *BMG*; rather, it applied the more lenient, *bona fide* claim test required by Court of Appeal in *BMG*. In making its decision, the Court analyzed s. 7(3) of PIPEDA, related to the disclosure of personal information when required to comply with a subpoena. Citing the Court of Appeal in *BMG*, Shore J. held that only a bona fide claim was needed and while making sure that caution be exercised by courts when ordering the disclosure of identities, in order to make sure that privacy is invaded at the least[399].

With regard to Rule 238 of the Federal Courts Rules, the Court found that the ISPs had relevant information for the claimant, given that without their help Voltage Pictures could not know the names and addresses of the defendants. The Court also explained that it would be unfair not to allow the plaintiff to obtain that information and that anyway ISPs would not incur in any cost, since Voltage Pictures agreed to

[394] *Voltages Pictures LLC v. Jane Doe and John Doe*, 2011 FC 1024 [*Voltage Pictures*].
[395] See Voltage Picture's website: http://www.voltagepictures.com/about.aspx.
[396] See M. GEIST, *Hurt Locker File Sharing Suits Come North: Federal Court Orders ISPs to Disclose Subscriber Info*, September 9, 2011, at http://www.michaelgeist.ca/content/view/5999/125/.
[397] *Voltage Pictures*, paras. 2-6.
[398] *Voltage Pictures*, par. 7.
[399] See *BMG II*, paras. 41-42.

reimburse any reasonable expense in which they might incur[400]. The claimant asked for "the minimum information necessary to allow it to assert its rights against the defendants to be disclosed to it"[401].

As a result of its reasoning, the Court granted the motion, giving two weeks to ISPs to provide the plaintiff with the information.

A main difference between the *Voltage Pictures* suit and the BMG case is that in the latter no ISPs contested the motion requested by the claimant[402]. Furthermore, *in Voltage* Pictures, the P2P users downloaded a movie and not a song. This is an important distinction, for the private copying exemption of section 80(1) only applies to music.

3.3.6 Critiques and comments on BMG

The *BMG cases* have drawn some attention from scholars, despite (or maybe because of) the fact that it has basically been the only suit regarding the conflict between copyright and personal data protection for years[403]. Even if the cases reached the stated goal of protecting users' personal data against the disclosure, the solution given by both courts left some questions unanswered.

First of all, the decisions bring out the fact that all the parties agreed on two points: "ISP account holders have an expectation that their identity will be kept private and confidential. This expectation of privacy is based on both the terms of their account agreements with the ISPs and sections 3 and 5 of the Personal Information Protection and Electronic Documents Act"; and "the exceptions contained in PIPEDA apply in this case and an ISP by virtue of s. 7(3)(c) of PIPEDA may disclose personal information without consent pursuant to a court order"[404]. In particular, the Federal Court of Appeal, asking for a *bona fide* claim threshold, lowers the requirements to be met for the disclosure of the information. The judges even stated that, once a plaintiff shows a *bona fide* claim that somebody is infringing

[400] *Voltage Pictures*, paras. 18-26.
[401] *Voltage Pictures*, par. 28.
[402] *Voltage Pictures*, par. 29.
[403] See, among others, BAILEY, *The Substance of Procedure*, cit.; I. KERR, A. CAMERON, *Nymity, P2P & ISPs: Lessons from BMG Canada Inc. v. John Doe*, in K.J. STANDBURG, D. STAN RAICU (eds.), *Privacy and Technologies of Identity: a Cross Disciplinary Conversation*, New York, 2006, 269; WILKINSON, *Battleground between new and old orders*, cit., 227.
[404] *BMG I*, par. 9.

her copyright, she has a *right* to have the infringer's identity revealed[405]. Despite the fact that the Court stated right away that "caution must be exercised by the courts in ordering such disclosure, to make sure that privacy rights are invaded in the most minimal way"[406], the attitude seems to be different from other cases, such as *Tariff 22*[407]. In the latter case, delivering his dissenting opinion, Justice LeBel stressed that the privacy of individuals would be directly implicated if the copyright owners could collect their data from ISPs. In his opinion, therefore, courts should be cautious in applying a test that could stimulate the monitoring of users' data[408].

It has been pointed out that, despite the reliance by the judges in the BMG decisions on cases with similar facts, tensions and principles, all those decisions were taken before the approval of PIPEDA[409]. The difference is especially crucial when taking into consideration the *Glaxo Wellcome* case. As previously illustrated, in this case plaintiffs were seeking production of documents in the possession of a public institution. Public institutions are governed by access legislation, in particular by the *Access to Information Act*[410]. As the same Act states, its purpose is "to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public"[411]. Furthermore, the case of *Glaxo Wellcome* was related to information held by a corporate person, while PIPEDA focuses only on individuals. For these reasons, it has been said that the reliance on *Glaxo Wellcome* by both courts was "entirely misplaced"[412]. Last but not least, the existence of PIPEDA at the time *BMG* was decided might or even should have rendered inapplicable the older cases to these ones[413].

Another important point which has been underlined is that there seems to be a difference between the concept of privacy on the one hand and the concept of data

[405] *BMG II*, par. 42.
[406] *Ibidem*.
[407] WILKINSON, *Battleground between new and old orders*, cit., 237.
[408] *Tariff 22 Supreme Court*, par. 155. LeBel J also hold: "Insofar as is possible, this Court should adopt an interpretation of s. 3(1)(*f*) [*of PIPEDA*] that respects end users' privacy interests, and should eschew an interpretation that would encourage the monitoring or collection of personal data gleaned from Internet-related activity within the home", see *Ibidem*, par. 153.
[409] WILKINSON, *Battleground between new and old orders*, cit., 261 ff.
[410] *Access to Information Act*, R.S.C. 1985, c. A-1.
[411] *Access to Information Act*, art. 2(1).
[412] WILKINSON, *Battleground between new and old orders*, cit., 244.
[413] WILKINSON, *Battleground between new and old orders,* cit., 262.

protection on the other hand. The two realms overlap only partially, as we can consider personal data protection as one of the many existing ways to protect privacy itself. Privacy, which one could summarize with the old famous sentence "the right to be let alone", relates to a much broader range of interests than data protection does. The latter one pertains only to the way data are handled, how they are gathered, managed, diffused and so on. On the contrary, privacy seems to be more concentrated on *whether* information can or cannot be gathered[414]. As a consequence, one should be careful in exchanging the two words, since they contemplate quite different ideas[415].

Even without considering these differences, more than one author has expressed concerns about the solution given in BMG. As already said, the results reached in the two decisions, even if practically protecting John Does' data (and correlated privacy), left some issues unresolved. As mentioned, both levels of the Federal Court would have ordered the disclosure of the data had the plaintiffs met the evidentiary requirements or even if they simply were up-to-date. This means that in the future, CRIA or any other similar organization could obtain what at that time was denied. This might probably be in contrast with the Charter of Rights and Freedoms which, despite not directly mentioning information privacy, comprises some privacy-related provisions. It has been suggested that cases like *BMG* should be solved by looking at the Charter of Rights and Freedoms. Indeed, even if the Charter applies only to state activities, the common law should not grow in contrast or even inconsistently with the Charter itself[416]. As mentioned earlier in this chapter, the Supreme Court has indeed also stated that privacy has a place in the Charter, in

[414] WILKINSON, *Battleground between new and old orders*, cit., 244-246, *sic passim*.

[415] The borders between the two and the gray areas in which they overlap have been the object of many interesting studies, which, anyway will not be recalled here. An interesting reconstruction for the Canadian system is given by prof. Wilkinson. She argues that the "characteristics of personal data protection differentiate it from legislation and common law which have arisen in defence of privacy rights. […] these statutes [*meaning: those regarding personal data protection*], since they do not deal with the right to require and individual to disseminate information to particular organizations, but do limit the scope of the organization's abilities to use the information collected from individuals about themselves and prohibit its further dissemination except in very strict circumstances, appear to be extensions of the law of confidentiality, rather than privacy statutes", see WILKINSON, *Battleground between new and old orders*, cit., 256.

[416] See A. MIN CHEE-FONG, *Unmasking the John Does of Cyberspace: Surveillance by Private Copyright Owners*, 4 CJLT 169 (2005), 176, citing *Retail, Wholesale and Department Store Union, Local 580 v. Dolphin Delivery Ltd* [1986] 2 S.C.R. 573 at par. 32 ff. Nevertheless the same decision clearly stated that the Charter does not apply to private litigation.

particular in Section 8 regarding the right to be secure against unreasonable search or seizure and Section 7 related to life, liberty and security of citizens.

The possible extension of personal data protection into the private sector appears to be an important factor for the interests at stake[417]. Had the court solved the cases in a different way, a possibility other than obtaining the information with a third-party discovery in a civil case would have been to commence a criminal process against the same Does. Criminal law is differently perceived from private law. "In the case of criminal proceedings, the public interest is much clearer than in disputes between private parties in civil proceedings"[418]. Or at least it *should* be[419]. In the decision *R. v. Plant*, the Supreme Court assessed a test for the reasonable expectation of privacy in criminal cases. The test included these factors: "the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated"[420]. Moreover, already in 1984, in the decision *Hunter v. Southam Inc*., the Supreme Court clarified that the state's interest in preventing crimes can prevail over the individual's interest to privacy when credibly-based probability replaces suspicion[421].

As has been highlighted in describing the US context, it is also the case in the Canadian system that there is the need for a balance between a copyright holders' right to obtain protection against the infringement of their works and a users' right to personal data protection and/or privacy. In order to reach a correct balance between them, it seems essential to understand their inner nature and their public values[422]. Should a purely economic right (such as the one of the major record labels) prevail against a "personal" right such as the privacy of users? Some authors have classified

[417] WILKINSON, *Battleground between new and old orders*, cit., 265-266.
[418] WILKINSON, *Battleground between new and old orders*, cit., 264. This is also because in criminal proceedings there is necessarily a state action and therefore Charter applies.
[419] Many scholars have stressed the dramatic increase of the use of criminal remedies in provinces where other kind of remedies would have been anyway effective. This inevitably leads to the decrease in the valuation of criminal law and, consequently, in the compliance with the same. For an idea on the issue see, among the first contributions on overcriminalization, H.S. KADISH, *The Crisis of Overcriminalization*, 374 *The Annals of the American Academy of Political and Social Science*, 157, 1967.
[420] *R. v. Plant*, cit., par. 26.
[421] *Hunter v. Southam Inc*., cit., par. 40.
[422] BAILEY, *The Substance of Procedure*, cit., 635.

this counterbalancing as a matter of fairness[423]. But in my view fairness is a culturally-oriented value[424]. Therefore, in balancing rights, courts may more or less explicitly and more or less unconsciously take into consideration "culture"[425]. This is true also in relation to the "ranking" of rights and the subsequent balance[426].

Undoubtedly, for modern societies the creation and dissemination of ideas is of extreme importance. These ideas should be protected by intellectual property rights. At the same time, our societies consider the security of privacy as an essential right, perhaps even more important than intellectual property protection[427]. However, even if in the Canadian system the problem of protecting anonymity has emerged, no case has appeared to have taken into account this fuller account of privacy[428]. In this sense, BMG can be thought as a first step towards such a deeper account of privacy, perhaps as a result of the participation of an organization like CIPPIC. At least the judges gave indications as to the need to keep the data disclosed to a minimum and accepted that data should be protected with some types of anonymity and the expectation was that it should be thus[429].

All in all, the Canadian approach, even if seen as requiring the lower, *bona fide* threshold as the DMCA section 512(h), does seems to better protect privacy, due to the different construction of the test applied[430]. The requirement of current and complete evidence is surely a barrier to the disclosure of data and at the same time the ISPs have demonstrated a reluctance with supplying CRIA with information that could have led to a breach of the obligation deriving from PIPEDA with respect to their customers[431]. Nonetheless, some meaningful problems remain. One could never possibly know whether the person linked to the IP number was in fact the infringer. Furthermore, once anonymity and/or privacy are violated, the revelation is final. But,

[423] See for example the analysis made by L.B. SOLUM, *Procedural Justice*, 78 S. Cal. L. Rev. 181 (2004), 258-259.
[424] Some societies find fair to kill someone who enters someone else's property or that kills another person. Other societies do not.
[425] Culture meant in the sense of social perception of happenings.
[426] SOLUM, *Procedural Justice*, cit., 259 talks about rights ranked in a "lexical ordering".
[427] KERR, CAMERON, *Nymity, P2P & ISPs: Lessons from BMG Canada Inc. v. John Doe*, cit., 288.
[428] BAILEY, *The Substance of Procedure*, cit., 638. But see WILKINSON, *Battleground between new and old orders*, cit., 234 ff., who mentioned *Tariff 22 Supreme Court* as a decision where privacy concerns were raised.
[429] *BMG I*, paras. 44 ff.
[430] BAILEY, *The Substance of Procedure*, cit., 640.
[431] See for example *Shaw's Written representations*, 17.

at the same time, individuals' anonymity and/or privacy could be compromised even if those individuals did not engage in any illegal activity, because acting, for example, within a fair dealing (or fair use) exemption[432].

To be fair, there have been also contrary opinions. For example it has been argued that one cannot expect privacy on her name: "if a person's name has a freestanding expectation of privacy, then no one will be held accountable for his or her actions as no prosecution could issued in the person's name without consent" and "there is […] no freestanding right to be immune from lawsuit" [433]. This is certainly true, but the same author gives herself an answer: privacy has to be protected when an individual's activity is personal in nature or potentially embarrassing. Moreover, Canadian courts and administrative bodies have expressed the opinion that even general web-browsing habits can be considered personal[434].

As already mentioned, users have an expectation that their data will be kept confidential. One can imagine different kinds of data which a user would prefer not to disclose. In addition to the strictly identificatory data, two other categories of information have been at least identified. The first is related to the files on the user's computer that are accessible by others through the network; the second, and indeed closely linked to the first, refers to the files actually exchanged among users[435]. It has been argued that there should be no difference in handling data related to – for example – music and data related to religion[436].

As seen, this data can be discovered also by interested third parties (such as CRIA), while the first one is only known by the ISP. "ISPs have increasingly become

[432] BAILEY, *The Substance of Procedure*, cit., *sic passim* 639-642.
[433] Thoughts and quotations from YIU, 64.
[434] See for example the dissenting opinion of LeBel J. in a case before the Supreme Court, which stated that web surfing and downloading "habits tend to reveal core biographical information about a person" (*Tariff 22 Supreme Court*, par. 155). The Canadian federal Privacy Commissioner had the same opinion in a case where a broadcaster was accused of collecting personal data through a Web site, see PIPEDA Case Summary #2001-25 – *A broadcaster accused of collecting personal information via Web site* – at http://www.priv.gc.ca/cf-dc/2001/cf-dc_011120_e.cfm.
[435] MIN CHEE-FONG, *Unmasking the John Does of Cyberspace: Surveillance by Private Copyright Owners*, cit., 170-171.
[436] A. CAMERON, *Learning from data protection law at the nexus of copyright and privacy*, in I. KERR (ed.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society,* Oxford, 2009, 59-60. Although I do not completely agree with this statement, I endorse the wider vision of the Author.

trusted holders of and gatekeepers to our personal information"[437]. With regard to this matter, it would be no surprise if one user sued her ISP for a breach of fiduciary duties[438]. ISPs usually include one or more provisions regarding the respect of users' privacy in the contract with their clients[439]. Therefore users have an expectation that their confidences will remain secret. Indeed, at this point it would be more a matter of confidence than of privacy. It has been pointed out that the border between personal data protection and confidence is uneasily understood and, even worse, the two concepts overlap and substitute those of privacy. This obviously created even more confusion than already existing[440].

Even if this is not directly connected to the *BMG* case, it is worth noting that in 2009 the Canadian Radio and Telecommunications Commission (CRTC) imposed a different and higher standard of protection for the personal information collected by ISPs[441]. This policy aims at balancing the right of Canadians to use the Internet for their purposes whit the interest of ISPs to manage the traffic generated in their networks. This different approach to privacy was adopted in response to the concern showed through a public consultation process[442].

Furthermore, the Privacy Commissioner of Canada stated that a *subpoena duces tecum*, such as those initially used by the RIAA in USA, would not be a sufficient basis, in and of itself, for the disclosure of personal information in those documents without the consent of the individual as a subpoena does not compel

[437] KERR, CAMERON, *Nymity, P2P & ISPs: Lessons from BMG Canada Inc. v. John Doe*, cit., 272. The authors feared that this role of ISPs would cease in case the intermediaries would be reimbursed for the costs deriving from the information search and revelation. The "cost issue" was recalled in each and every ISPs' written representation.

[438] KERR, CAMERON, *Nymity, P2P & ISPs: Lessons from BMG Canada Inc. v. John Doe*, cit., 273. For an interesting analysis of the relationship between ISP and users see I. KERR, *The Legal Relationship Between Online Service Providers and Users*, 35 Can. Bus. L.J. 419 (2001).

[439] Many Canadian ISPs are members of the Canadian Association of Internet Providers (CAIP) and endorse its privacy code: CAIP Privacy code available at: http://www.cata.ca/communities/caip/codeofconduct/privacycode.html. Actually, this code do not really seems to improve the conditions already exiting thanks to PIPEDA, see MIN CHEE-FONG, *Unmasking the John Does of Cyberspace: Surveillance by Private Copyright Owners*, cit., 175.

[440] WILKINSON, *Battleground between new and old orders*, cit., 253 ff.

[441] See Canadian Radio and Telecommunications Commission (CRTC) *Review of the Internet traffic Management Practices of Internet Service Providers*, Telecom Public Notice 2008-19, October 21, 2009, at par. 102 available at http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm.

[442] A. CAMERON, CRTC *Imposes Super-PIPEDA Privacy Protection for Personal Information Collected by ISPs*, 10 I.E.C.L.C. 94 (2009).

actual production[443]. And we must not forget that the same Privacy Commissioner has stated more than once that IP addresses are indeed personal information[444].

What courts in Canada have not considered is that privacy may be part of the Charter of Rights, while copyright is not. This could be a light to be followed in balancing these two rights, which at the very end means balancing copyright holders' and users' rights[445].

[443] See PIPEDA Case Summary n. 2009/05 – *Husband's financial information disclosed to wife's lawyers by accounting firm improperly complying with Summons to Witness*, available at http://www.priv.gc.ca/cf-dc/2009/2009_005_0223_e.cfm

[444] See supra note n. 574.

[445] HAGEN, ENGFIELD, *Canadian Copyright Reform: P2P Sharing, Making Available and the Three-Step Test*, cit., 501. The same Authors, however, acknowledge that "[i]t could be argued that the Federal Court does not ignore *Charter* rights when copyright conflicts with rights of expression and privacy because, first of all, *Charter* rights do not cover actions which infringe copyright and second, as some previous jurisprudence suggests, a *prima facie* infringement of *Charter* rights by copyright may be justified under section 1 of the *Charter*", which "guarantees the rights and freedoms […] only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".

Chapter 4
The Italian System

4.1 The legal framework of file sharing

The basis on which stands the entire regulation of the Italian *diritto d'autore* is the *Legge* 22.4.1941 n. 633. This statute, which has undergone a massive number of amendments, nevertheless maintains its original systematic and includes almost all the provisions related to copyright. Amendments have often been the product of interventions of the European Union[1]. In fact, despite the Treaty establishing the European Economic Community of 1957 does not directly consider copyright, art. 30 of the same Treaty allowed restriction to free circulation of goods and services for the protection of industrial property[2]. This provision has been seen as a glimmer through which Europe could intervene, more and more often, in this strategic sector[3].

The Italian copyright legislation recognizes both the economic and the moral part of copyright. The economic right can be waived and it is limited in time, while the moral right is endless and is not alienable[4]. Art. 1, L. 633/41 proclaims that the protection goes to all the creative works belonging to literature, music, figurative arts, architecture, theater, and cinematography, regardless the form or way of

[1] Just to give some examples, deep modifications occurred with L. 18.8.2000, n. 248, the so called "anti-piracy law". To implement European Directive 98/71/EC on legal protection of designs, L. 633/41 was modified by d.lgs. 2.2.2001, n. 95. It was also amended by d.lgs. 9.4.2003, n. 68, which applied Directive 2001/29/EC, on the harmonisation of certain aspects of copyright and related rights in the information society. Among others, it is worth mentioning the innovations introduced by d.lgs. 16.3.2006, n. 140, introducing European Directive 2004/48/EC, on the enforcement of intellectual property rights, which will be of particular importance for this work.

[2] From 1st December 2009, date of entry into force of the Lisbon Treaty, The title of the "Treaty establishing the European Community" is replaced by "Treaty on the Functioning of the European Union" (TFEU) and the numbering of the two treaties has been changed. The current numbering of art. 30 is art. 36.

[3] Europe has even create an "Information Society and Media-*Directorate General*", which created a Digital Agenda for Europe. The mission of this Directorate is to achieve a digital single market; reinforce Europe's competitiveness by increasing ICT research and innovation; promote the access and use of ICT; implement the European legislation in the area of information society and media. Cf. the Directorate's website at url: http://ec.europa.eu/dgs/information_society/see_more/index_en.htm#mission.

[4] Cf. art. 20, L. 633/41 under which, regardless of exploitation rights, and even after having waived them, the author keeps the right of paternity of the work, and the right to oppose to any deformation, mutilation or any other modification, or damage against the work, which could prejudice the honor or the reputation of the author. Moral rights are regulated by arts. 20-24 of L. 633/41.

expression[5]. The second part of the article now provides protection also for softwares, which are considered literary works according to the Berne Convention[6], as well as for those databases which, as a choice of the author or for the particular disposal of the material, can be considered as an intellectual creation.

From the text of art. 1, it can be understood that protection is provided only for those works which can be considered "creative", meaning that there is a personal contribution of the author, regardless of its importance, so that the work shows a *quid novi* if compared to already existing works[7].

Parallel to L. 633/41, also the Italian civil code (c.c.) contemplates a few articles concerning intellectual property works. Among them, art. 2575 c.c. provides that are subject to copyright those intellectual creative works belonging to science, literature, music, figurative arts, architecture, theater, cinematography, regardless of their way or form of expression. As it can be easily noted, the wording of this article is essentially the same of art. 1, L. 633/41[8]. Art. 2575 c.c. is considered as an open provision for the protection of works of intellectual creation[9].

Legal protection can be accorded only to those works which are exteriorized: a work is protected only when "comes into the world". Art. 2, L. 633/41 contains a list of works which are protected by copyright. In particular, number 2 of the mentioned article includes musical compositions and works, with or without words, music dramas, and those music variations which constitute original works. The list contained in art. 2 is considered by the majority of the scholars as a mere exemplification of the protectable works[10].

---

[5] There are therefore two requirements for a work to be protected: the "creative character" and its affiliation to "literature, music, figurative arts, architecture, theater, and cinematography". Cf. N. ABRIANI, G. COTTINO, M. RICOLFI, *Diritto industriale*, in *Trattato di diritto commerciale diretto da Cottino*, Volume II, Padova, 2001, 360.

[6] Ratified and executed in Italy with L. 20.6.1978, n. 399.

[7] A. SIROTTI GAUDENZI, *Il nuovo diritto d'autore. La tutela della proprietà intellettuale nella società dell'informazione*, Sant'Arcangelo di Romagna, 2008, 39. Cf. the decision of the Italian Supreme Court: Cass. civ., 12.3.2004, n. 5089, in *Riv. dir. Ind*., n. 6/2005, 327 with commentary by G. DALLE VEDOVE and L. CHIAVEGATTI; in *Dir. Industriale*, n. 2/2005, 237 with commentary by G. BONELLI. For a deeper analysis of art. 1, see P. MARCHETTI, L.C. UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, Padova, 2007, 1487 ff.

[8] The Italian Civil Code is in fact subsequent to L. 633/41, given that the Code was enacted with R. D. 16.03.1942, n. 262.

[9] SIROTTI GAUDENZI, *Il nuovo diritto d'autore*, cit., 61.

[10] SIROTTI GAUDENZI, *Il nuovo diritto d'autore*, cit., 64 sustains that the list gives only some examples of what is copyrightable. The same interpretation can be found in P. GRECO, P. VERCELLONE, *I diritti sulle opere dell'ingegno*, in *Trattato di diritto civile italiano redatto da diversi giureconsulti sotto la*

As to the patrimonial rights, L. 633/41 specifies a list of rights connected to the protected work[11]:

- right to publish the work (art. 12);
- right to reproduce into many copies (art. 13);
- right to transcript the oral work (art. 14);
- right to execute, represent or play in public (art. 15);
- right to communicate (art. 16);
- right to distribute (art. 17);
- right to elaborate, translated and publish collective works (art. 18);
- right to rent and to loan (art. 18*bis*).

All these rights have a limitation in time, since they extinguish 70 years after the author's death[12].

Art. 12 considers the right to publish the work for the first time. It is considered as a first publication the first act of exploitation of the work. In fact, publishing does not only mean to print the work, but also a performance or another kind of diffusion, provided that this is made in front of the general public. With this right, the author can stop other persons from publishing her work[13]. Under the second part of this article, the authors have also the exclusive right to economically use the work in any form or way, whether original or derivative, within the limits of L. 633/41, specially with reference to the other exclusive rights[14].

Art. 13 provides for the exclusive right to reproduction. The provision was modified, among others, also by d.lgs. 9.4.2003, n. 68, which implemented European Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society. The prior formulation considered as

direzione di Filippo Vassalli, Torino, 1974, 55. MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1501, consider in their book a number of non-listed works, which are nevertheless protected by L. 633/41.

[11] This list is not closed, but just a list of examples, see MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1530. In the opinion of GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 130, the listed rights are just different ways of manifestation of a unique right: the right to economic exploitation.

[12] Arts. 25 ff., L. 633/41 provide the criteria to calculate the duration of the rights and the point from which the duration starts to run.

[13] GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 123-124.

[14] Given this second part of the article, some authors have question whether the right of art. 12 has its own content compared to the subsequent rights or not. See ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 412.

reproduction the multiplication of the work with any means, among which hand copy, print, lithography, recording, photography, cinematography, and any other technical mean with which it could be possible to make a copy of the work[15]. The norm did not therefore list an exclusive number of types of reproduction; rather, it enlarged the right to every technology suitable to reproduce the work of authorship. The current formulation is even wider. In fact, in order to implement the mentioned Directive, d.lgs. 68/03 introduced a extension of the right. The present wording of art. 13 describes the right to reproduction as the right to copy the work *directly or indirectly, temporary or permanently, totally or partially, in any way or form*, including hand copy, print, lithography, recording, photography, cinematography, and any other technical mean with which it could be possible to make a copy of the work[16].

This amendment was necessary to update the discipline to the reproduction obtainable trough digital technologies. Some scholars argue that, even if it was already intelligible in the previous wording, this modification clarifies the applicability of this article to digital copies. As a consequence, the download of a song from the Internet is to be considered as a reproduction[17]. Nevertheless, there are some exceptions and limitations to the right to reproduction, listed in art. 9, d.lgs. 68/03, amending L. 633/41[18]. As an example, let us consider the exception which is most related to this work. Art. 71*sexies* contemplates "private reproduction for personal use". The article allows the private reproduction of phonograms and videograms on any kind of support, made by a person for an exclusively private use, as long as there is no profit-making scope and without direct or indirect market aims[19].

[15] For an analysis of the previous text of art. 13, see ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 414-421. See also MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1548 ff, and in particular, on the single types of reproduction see 1550 ff.
[16] Emphasis added.
[17] SIROTTI GAUDENZI, *Il nuovo diritto d'autore*, cit., 81.
[18] Cf. arts. 65 ff., L. 633/41.
[19] Cf. art. 71*sexies*, co. 1, L. 633/41. See GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 167 ff. for the original regulation of reproduction for private use. For a deep analysis see MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1698 ff.

The right to reproduce is independent from the right of publication or of distribution; this means that the right is violated as soon as an unauthorized copy is made, regardless of whether the copy will be later commercialized or not[20].

Art. 15, L. 663/41 contains the rights to execute, perform or play in public. More precisely, this exclusive right concerns the execution, performance or play, in whatever way they are made, free of charge or for payment, of a musical work, of a dramatic work, of a cinematographic work, or of whichever work of public show, as well as of an oral work. The same article provides that it cannot be considered as public an execution, performance or play made within the ordinary family circle, the boarding school, the school or the nursing home, as long as it is made without profit-making scopes. In order to understand whether the execution is made within a family, a qualitative criterion should be applied[21].

From the text of art. 15 it can be inferred that there are three different forms of communication of the work, which are considered "performing rights":

1. execution: it comprises the communication of different types of works, in particular musical composition, regardless they contain a text or not, as long as there is no scenic action[22];
2. performance: it is the communication of the work through a scenic action;
3. play: it should be considered as the simple telling of a literary work, without a scenic action[23].

Art. 16 concerns the right to communicate. In particular, the previous wording of the article included the right to "diffuse" a work through means such as

[20] GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 133; ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 415; MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1551.

[21] See GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 138-139. On this definition see also MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1561-1562.

[22] ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 436-437.

[23] SIROTTI GAUDENZI, *Il nuovo diritto d'autore*, cit., 85. See also GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 135 ff. It is often very difficult to make a distinction among these activities, see the examples given in ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 437. The Italian *Corte di cassazione* held that the author of a musical work, not only posses the exclusive right to execute, perform and reproduce her work. She also has the right to diffuse it with distance means such us radio or television, cf. Cass. pen., 18.10.1999, n. 12820, in *Cass. pen*., 2001, 620.

television, radio, telegraph and so on[24]. The article has now a different text, due to the amendments introduced by d.lgs. 68/03. Art. 16 currently regulates the exclusive right to communicate to the public, introducing therefore a wider and more complete provision. The exclusive right regards wired or wireless communications of the work, through distance means such us those contemplated by the previous regulation. The article also comprises communication via satellite, cable rebroadcasting, as well as communication to the public with particular access conditions. Furthermore, the article includes what has been called "interactive communication"[25], that is the making available of the work so that everyone can have access to it where and when individually decided[26]. Thus, art. 16 includes every kind of communication made when the public is not physically present, including file-sharing and streaming[27]. The second part of the article clarifies that this right does not exhaust itself with any of these kinds of communication, including the act of making available[28].

The subsequent article considers the right to distribute the work with or without profit making aims[29]: it is the right to commence the commercialization of a work, i.e. the exclusive right of the author to the economic exploitation of her creation. Also art. 17 was modified by d.lgs. 68/03, which widened the applicability of the right. The current text considers the right to put the original work on the market or in circulation, or to make anyway available it to the public, with whatever means and at whichever title.

This right is the one which gives the author the power to prevent the transfer of the ownership and of the exploitation rights, as well as the making available of the

[24] For a comment on the older formulation, see GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 141 ff.; ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 440 ff, commenting also the provision of the WIPO Treaties, later implemented in Italy.
[25] MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1566.
[26] Art. 16*bis* supplies the definition to understand art. 16. ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 445 claim that "somehow, *diritto d'autore* is going from copyright to accessright".
[27] Cf. MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1566-1567, that also give an account of the different interpretations for this article and their implications.
[28] The right to make available was introduced by d.lgs. 68/03 as an implementation of Directive 2001/29.
[29] In the past this right was related only to distribution with profit aims; cf. ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 422; GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 150 ff.

work through, for example, loan[30]. The article also contemplates the so called "exhaustion principle", close to the "first sale doctrine", for the case that the author decides to definitely put her work on the market[31]. The right to distribute the work does not exhaust itself within the European Community, unless the first act of sale or act of transfer is made either by the right holder or with her consent. This provision is not applicable when the making available of the work is made in a way by which everyone can have access to it from a place and at a time individually chosen by the user, such as in the case of watching a movie in streaming on the web.

As mentioned at the beginning of this paragraph, the Italian copyright legislation has been deeply modified by the implementation of European Directives. We will briefly consider here some of the most important directives enacted starting by the year 2000, which are relevant for the aims of this research: the reference is to Directives 2000/31, 2001/29 and 2004/48.

The first of these European laws is Directive 2000/31/EC "on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market" (so called "Directive on electronic commerce"), implemented in Italy with d.lgs. 9.4.2003, n. 70. The intervention on electronic commerce probably seemed to be the most appropriate and more justifiable point where to start with the reorganization of Member States' legislation on intellectual property.

The main innovation that this Directive and, consequently, d.lgs. 70/03 introduced is the regulation of internet service providers' liability. In accordance with the different roles that an ISP can have in the virtual world, the Directive states when and how they can be considered liable for the violation committed by themselves or by a third party. The Italian transposition of this Directive has been criticized for being a sort of "copy-paste" of the European text[32]. In particular, d.lgs.

[30] ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 423.

[31] GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 151 explain that once the commercialization of the copy has been made, this right is exhausted. This means that subsequent acts of sell are perfectly licit for those who bought the copy directly from the person who legitimate introduced the copy into the market. See also ABRIANI, COTTINO, RICOLFI, *Diritto industriale*, cit., 423 ff; MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1572-1574.

[32] See for example G.M. RICCIO, *La responsabilità degli* Internet providers *nel d.lgs. n. 70/03*, in *Danno e Resp*., n. 12/2003, 1157, spec. 1158 ff.; G. SPEDICATO, *Postille in tema di responsabilità extracontrattuale del* provider *alla luce del recente Decreto Legislativo n. 70/2003*, in *Ciberspazio e diritto*, n. 3/2003, 155-156.

70/03 lists the mentioned activities of ISPs, faithfully following the nomenclature given by Directive 2000/31[33].

The three main activities considered are "mere conduit", "caching", and "hosting". As we will see, there is also a sort of "safe harbors" system, such as the one introduced by the DMCA in the United States. The more the ISP is involved in the activity made by users on the web, the higher is the probability for the ISP of being liable and the more difficult is to prove its innocence in the illicit action.

Art. 12 of the Directive, implemented by art. 14, d.lgs. 70/03 considers the activity of "mere conduit" as "the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network". In this case, the national legislation implementing the directive had to "ensure that the service provider is not liable for the information transmitted, on condition that the provider: a) does not initiate the transmission; b) does not select the receiver of the transmission; and c) does not select or modify the information contained in the transmission".

Art. 13 of Directive 2000/31, transposed in art. 15 of d.lgs. 70/03, describes the function of "caching providers", as "the transmission in a communication network of information provided by a recipient of the service". In this case, Member State had to implement a regulation which ensures that the ISP is not liable for the automatic, intermediate and temporary storage of data, as long as it is performed for the only purpose of making more efficient the information's transmission to other recipients of the service, when requested. This exemption from liability can be obtained under the condition that "a) the provider does not modify the information; b) the provider complies with conditions on access to the information; c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry; d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of

[33] For a deep analysis of the Italian regulation of ISPs' liability, and further bibliography, see G.M. RICCIO, *La responsabilità civile degli* internet providers, Torino, 2002; M. GAMBINI, *Le responsabilità dell'Internet* service provider, Napoli, 2006; M. DE CATA, *La responsabilità civile dell'Internet* service provider, Milano, 2010.

the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement".

The activity of "hosting" is defined by art. 14 of Directive 2000/31 and by art. 16 of the Italian decree implementing it. Hosting "consists of the storage of information provided by a recipient of the service". For ISPs providing this service, Member States had to implement a regulation which preserves the service provider from liability for information stored at the request of a customer, as long as "a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information"[34]. The second part of the provision ensures that this rule does not apply when the customer is acting under the authority or under the control of the intermediary.

The liability system for ISP is completed by the provision of art. 15 of the Directive (art. 17, d.lgs. 70/03), on the absence of a general obligation to monitor, with the obvious aim to avoid the infamous "chilling effect". In particular, the Directive ensured that national legislations did not impose a general obligation on intermediaries, providing the services covered by the three preceding articles, to monitor the data they store or transmit, let alone a general obligation to actively seek illegal conducts. The same article nevertheless provides that Member States may establishes either: a) an obligation for ISPs to inform the competent public

[34] Even if, as mentioned, the Italian implementation of the Directive 2000/31 was a sort of copy-paste, art. 16, d.lgs. 70/03 contains a difference if compared to art. 14 of the Directive. In fact, letter e) of art. 14 exempts the provider from liability, as long as it "acts expeditiously to remove or to disable access to the information". The Italian version requires, instead, a further element, since this expeditiously removal should be done "upon the request of competent authorities". Italian scholars have interpreted the provision introduce by art. 16, d.lgs. 70/03 in many different ways. Some of them claim that the host provider should be considered liable only when both the conditions a) and b) are met; cf. for example L. BUGIOLACCHI, *La responsabilità dell'*host provider *alla luce del d.lgs. n. 70/2003: esegesi di una disciplina "dimezzata"*, in *Resp. civ. prev.*, n. 1/2005, 198 ff..; See also SPEDICATO, *Postille in tema di responsabilità extracontrattuale del* provider *alla luce del recente Decreto Legislativo n. 70/2003*, cit., 160-161. Other apply the two conditions, respectively to criminal and civil proceedings, for the different degree of knowledge required by the two branches of law to consider a person liable; cf. RICCIO, *La responsabilità degli Internet* providers *nel d.lgs. n. 70/03*, cit., 1162. Lastly, other authors consider the two conditions as being alternatives; cf. G. CASSANO, I.P. CIMINO, *Il nuovo regime di responsabilità dei* providers*: verso la creazione di un novello «censore telematico»*, in *Contratti*, n. 1/2004, 91 ff.

authorities of the existence of allegedly illegal conducts undertaken, or of information provided by customers; or b) an obligation to communicate, if requested by competent authorities, information enabling the identification of recipients of their service, with whom they have storage agreements.

Art. 17, d.lgs. 70/03 provides in its third part for a particular provision which is not considered by art 15 of Directive 2000/31. The Italian provision introduces another form of liability for the provider. In particular, the ISP will be liable in tort when, even if requested by the administrative or judicial authority, it did not promptly act to stop the access to the illegal contents. It will be also liable when, even knowing of the illicit or prejudicial nature of the contents to which the provider itself gives access, it has not informed the competent authorities[35]. This rule is not a direct implementation of an explicit provision of the directive; it derives from recital n. 48, according to which the directive did not affect the possibility for national legislators of requiring ISPs hosting information provided by recipients of their services to apply a duty of care, which could reasonably be expected from them, in order to detect and prevent certain illegal conducts.

With regard to what said so far, it is worth mentioning also L. 21.5.2004, n. 128[36]. Art. 1, co. 5, of this law provides that when required by a judicial authority's provision, ISPs have to communicate to policing authorities the data they hold, and which are useful to find website managers and authors of illicit conducts. Furthermore, it provides that, with regard to the violations done through the web and punished by the same law, ISP should make whatever possible to prevent the access to the contents or to remove the same contents. This rule does not apply to mere conduit providers and, in any case, it reserves the application of arts. 14-17, d.lgs.70/03.

Another fundamental intervention of the European Union in the field of intellectual property is Directive 2001/29/EC "on the harmonisation of certain aspects of copyright and related rights in the information society". Despite its title, the directive introduces a number of different innovations in the legislation of

[35] For an analysis of the problems in interpreting this article and for its relation with the previously summarized ones, see GAMBINI, *Le responsabilità dell'Internet* service provider, cit., 302 ff.
[36] This law, which is the consolidated version of d.l. 22.3.2004, n. 72 (so called "Urbani decree" from the name of the proposing minister), aimed at contrasting the unlawful diffusion of audiovisual materials, and at sustaining cinematographic and show businesses.

copyright, which do not only modify the look of this right in the information society, but also in the "analogical world". The European Union felt the need to intervene in order to reinforce and harmonize Member States' legislation concerning the control of copyright infringement [37]. This directive was thought as complementary to Directive 2000/31, and introduces injunctive relief against infringing activities. Furthermore, Directive 2001/29 was also the response of European Union to the implementation of WIPO Treaties of 1996[38].

As mentioned, Directive 2001/29 gave a new face to the main economic copyrights and neighbouring rights[39]. At the same time, the Directive also introduced a list of exceptions and limitations[40]. In particular there are four main areas in which the European legislation intervened: the right of reproduction[41]; the adaptation to the new technological landscape of the right to communicate to the public[42]; the protection of technological protection measures[43]; the right to distribute and the introduction of rules related to the exhaustion of the right[44].

An important novelty of Directive 2001/29, and consequently of d.lgs. 68/03, is the introduction of the "right to make available to the public", in order to adapt the right to communicate to the public to new technological developments. In particular, the European intervention implemented this right which was provided for by the

[37] Cf. recital n. 6 of Directive 2001/29: "Significant legal differences and uncertainties in protection may hinder economies of scale for new products and services containing copyright and related rights". See also the press release "Commission welcomes adoption of the Directive on copyright in the information society by the Council", of 21.4.2001, available at the url: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/528&format=HTML&aged=1&language=EN&guiLanguage=en, in which it can be read "he quality and quantity of private copying and the growth of electronic commerce all mean that there should be greater protection for rightholders in digital recording media (whereby unlimited numbers of perfect copies may be made rapidly). In certain limited cases, where rightholders have made the means available, private copying may be carried out".

[38] Cf. recitals n. 15 and 19 of Directive 2001/29. According to R. CASO, Digital Rights Management. *Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Padova, 2004, 157, the Directive went beyond what requested by the WIPO treaties, deeply reinforcing the protection of copyright, as already done by the DMCA.

[39] CASO, Digital Rights Management. *Il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit., 154, available as a digital reprint at http://www.jus.unitn.it/users/caso/pubblicazioni/DRM/Roberto.Caso_DRM.pdf.

[40] Art. 5 of Directive 2001/29.

[41] Cf. art. 2 of Directive 2001/29.

[42] See art. 3 of Directive 2001/29.

[43] Cf. arts. 6 ff. of Directive 2001/29. See SIROTTI GAUDENZI, *Il nuovo diritto d'autore*, cit., 323 ff.; P. MARZANO, *Diritto d'autore e* digital technologies. *Il* digital copyright *nei trattati OMPI, nel DMCA e nella normativa comunitaria*, Milano, 2005, 179 ff.

[44] MARZANO, *Diritto d'autore e* digital technologies. *Il* digital copyright *nei trattati OMPI, nel DMCA e nella normativa comunitaria*, cit., 24.

WIPO Treaties. More precisely, the Directive went beyond the request for protection made by the Treaties and extended the right also to broadcasting organizations. A fundamental element within the right to make available is the notion of "public", which has not been clarified neither in the text of the Treaties nor in the text of the Directive. Some scholars have considered, therefore, that this notion should be applied as interpreted when mentioned in national laws, nevertheless excluding the close family circle and closest social acquaintances[45]. In our system, as seen, art. 15, L. 633/41 provides an explanation for what should be considered public or not.

Following the WIPO Performance and Phonograms Treaty, through d.lgs. 68/03 the legislator introduces some exclusive rights for phonograms producers.

Actually, L. 633/41 has protected some rights of performers since its enactment (art. 80 ff.)[46]. This part of the statute has been deeply modified by d.lgs. 68/03. In particular, art. 72 now says that the phonograms producer has the exclusive right to authorize the direct or indirect, temporary or permanent, reproduction of her phonograms, in whichever way or form, totally or partially, and through whatever duplication process. The phonogram producer has also the exclusive right to distribute her phonograms, to rent and loan them, and to make available them "in such a way that members of the public may access them from a place and at a time individually chosen by them"[47]. This right has the limit of 50 years of validity from the moment of the fixation of the work or from the eventual legitimate publication of the work, when this is done later than the fixation (art. 75). The same rights are recognized also to the producers of films, for the same period of time (art. 78*ter*). Art. 79 considers also the same rights in favor of broadcasting organizations, meaning radio and television operators. Finally, art. 80 provides for the same right for performers, including actors, singers, musicians, dancers and all those people which perform, sing, play or tell or anyway give performance of works of authorships, regardless whether these works are under copyright or in the public domain.

The third important directive mentioned was enacted in 2004. Directive

[45] Cf. REINBOTHE, VON LEWINSKI, *The WIPO Treaties 1996: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty: commentary and legal analysis*, cit., 111.
[46] SIROTTI GAUDENZI, *Il nuovo diritto d'autore*, cit., 353 ff.
[47] This is the text of art. 3 of Directive 2001/29 on the "Right of communication to the public of works and right of making available".

2004/48 was thought to enforce intellectual property rights (so called "IPR enforcement directive"). The Directive was a response to the increasing threats posed by new technologies to intellectual property. Leaving the precedent directives unchanged, this one introduced only new process instruments to obtain the enforcement of industrial property rights. The Directive was implemented through d.lgs. 16.3.2006, n. 140, which greatly amended L. 633/41 in the part concerning copyright enforcement.

The two provisions which are of most importance for this work are art. 156 and 156*bis*. Both the provisions will be central in the decisions which will be later analyzed.

Art. 156 offers a tool to the copyright holder who fears the violation of her exploitation right, or who wants to prevent the perpetuation or repetition of a violation which has been already committed. The right holder can ask the judge to ascertain the violation and to enjoin the prosecution of the infringement to either the author of the violation or to the intermediary, whose services have been used to perpetrate the infringement.

Art. 156*bis* provides a tool for "discovery", meaning that it introduces in the Italian system an institution which is typical of common law systems[48]. When a party gives serious evidences, from which it can be inferred that its claims are sound, and the same party detected documents, elements or information held by the counterparty, which could confirm those serious evidences, it can ask the judge to order the exhibition or the disclosure of the information from the counterparty. The party can also ask the judge to order the counterparty to give elements for the identification of the individuals involved in the production and distribution of the goods or services which constitute the violation of the copyright. The same article also prescribes that when a judge applies one of these provisions, she should adopt suitable measures in order to grant the protection of confidential information, taking into account also the counterparty's observations.

Even if the wording of the article could be somehow misleading, this provision does not modify the regime of ISPs' liability. It only provides an instrument, in favor of copyright holders, to obtain the collaboration of ISPs in order

[48] MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1882.

to reach the enforcement of copyright[49].

After recalling briefly the Italian legislation on *diritto d'autore*, it is worth saying a few words on the regulation of music as a work of authorship[50]. As previously mentioned, art. 2, L. 633/41, lists which works are protected. Among them there are music works and music composing, with or without words, dramatic-musical works and those music variations which constitute original creations. Already in 1999, scholars claimed that, despite L. 633/41 does not expressly mention the use of computers as a mean for reproduction of music and the use of Internet as a mean for distribution, it would be no-sense to consider that Mp3 files are not covered by copyright legislation[51]. In any case, arts. 171, 171*ter* and 174*bis* represent the provisions mainly related to the protection of copyright in the web.

Art. 171*ter* has been the first provision punishing file-sharing. This article is quite controversial in its co. 2 letter a*bis*). It was originally introduced in 1994, but it was later subject to a number of amendments, which were mainly focused on setting the "aim" of the infringer's conduct[52]. The criminal provision punishes the infringer with imprisonment from one to four years and with a fine from about 2.500 to 15.500 euros. The punishable conduct consists in communicating a complete or partial copyrighted work to the public, through the introduction into telecommunication networks, using whichever kind of connection. This conduct shall be made in violation of the right to communicate to the public (art. 16) and with profit-making aims. In case the conduct is of particularly little importance, the punishment is diminished by the judge.

As said, the article had been modified many times. The initial wording asked for the existence of a "profit-making aim" ("*a fini di lucro*" in the Italian text). Later on, this aim was substituted with the aim of "gaining a benefit" ("*per trarne profitto*" in the original wording), but it was modified again, returning to the original version. The main difference between the two forms concerned the possibility to punish also

[49] SIROTTI GAUDENZI, *Il nuovo diritto d'autore*, cit., 367.
[50] Cf. GRECO, VERCELLONE, *I diritti sulle opere dell'ingegno*, cit., 62 ff. The authors, who wrote their book in 1974, interestingly considered the problems of the protection of music connected to the use of computers.
[51] A. MASSIMINI, *Cyberdiritto d'autore*, Napoli, 1999, 40.
[52] The article was introduced by d.lgs. 16.11.1994, n. 658, later modified by: L. 18.8.2000, n. 248; d.lgs. 9.4.2003, n. 68; L. 21.5.2004, n. 128 (consolidated version of "Urbani decree"); by L. 31.3.2005, n. 43.

the single user. In fact, usually the word "*lucro*" (meaning profit) is used for a commercial activity, such as the profit made by a company. According to some interpretation, the word "*profitto*" could instead be applied also to little gains, such those "earned" by end users who do not buy CDs and therefore can "gain these savings". This particular wording led to fluctuating decisions by the Italian *Corte di Cassazione*[53].

There is another provision which concurs in punishing file sharing along with art. 171ter. In fact, art. 171, co. 1, letter a*bis*) imposes a fine from about 50 to about 2.050 euros to the conduct of making a copyright work completely or partially available to the public, through the input of the work into a telecommunication network, without having the right to do so, regardless of the aim and of the form used to do so. This provision undoubtedly refers to peer-to-peer, but it considers only the introduction of the copyrighted work into the web and not the consequent sharing and diffusion[54].

The same article also provides a sort of "settlement" tool for a person who violated the provision mentioned above. In particular, this person can pay an amount of money as high as the half of the maximum of fine provided by the article (meaning about 1.025 euros), as well as the judicial fees. This payment extinguishes the crime[55].

Moreover, art. 174*bis* prescribes that parallel to the criminal punishment, those who violate art. 171, co. 1, letter a*bis*) are also punished with a fine as high as the double of the market price for the violated work, and in any case not less than 103 euros. When the price cannot be easily determined, the violation is punished with a monetary sanction between 103 and 1032 euros. This sanction is applied in

[53] See for example Cass. pen., 9.1.2007, n. 149, in *Dir. Internet*, n. 3/2007, 257 with commentary by D. TERRACINA; in *Guida al diritto*, n. 5/2007, 38, with commentary by A. SIROTTI GAUDENZI. In this case the Court considered that the word "*lucro*" had to be interpreted as a relevant economic gain. Therefore, the exchange of software for free, could not be considered as an economic activity, since it was not linked to any advertisement or other economic gain. On the point see A. DI AMATO, *Musica* on-line *e tutela penale*, in *Dir. Internet*, n. 4/2007, 329 ff; and more specifically D. TERRACINA, *Lucro e profitto nella giurisprudenza della Corte di Cassazione in materia di violazione del diritto d'autore e dei diritti connessi*, in *Dir. Internet*, n. 3/2007, 259.

[54] MARCHETTI, UBERTAZZI, *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, cit., 1937. For an explanation of the relationship between this provision and the one introduced by art. 171*ter*, co. 2, letter a*bis*), see *Ibidem*, 1958. The main difference is that art. 171, co. 1, letter a*bis*) pusished the "making available", while the other provision concentrates on "communication to the public" (see again *Ibidem*, 1968).

[55] Cf. art. 171, co. 2, L. 633/41, as modified by art. 3, d.l. 31.1.2005, n. 7.

relation to each item that has been duplicated.

There is also another rule which has been interpreted by scholars as a provision punishing illegal download[56]. Art. 174*ter* punishes with a monetary fine of 154 euros, and with the forfeiture of the material, those who, among other conducts, illegally uses, even if via ether or cable, duplicates, reproduces, totally or partially, with whatever process, works or materials which are protected by copyright. The punishment for this conduct cannot concur with those from art. 171.

As it can be understood by reading this paragraph, the whole Italian regulation of copyright has been undergoing a lot of changes, not only due to the European influence. The imposition of criminal penalty has been harshly criticized by scholars[57]. Nevertheless it denotes the will of protecting copyright as hardly as possible, even if this approach has not led to a decrease of the phenomenon to the extent the legislator would have hoped.

4.2 The legal framework personal data protection

In the Italian system the right to privacy emerged quite late, if compared to what had happened in the United States. The steps that led to the full protection of such a right consist in some important decisions taken by the *Corte di cassazione*. It was an escalation, starting in the Fifties with some small signals and going to the full acknowledgment of the right in the middle of the Seventies. Nevertheless, there was no unified protection for this right up to the Nineties, when comprehensive legislation on the issue was introduced[58].

[56] Among others see S. RICCI, G. VACIAGO, *Sistemi* peer to peer*: rilevanza penale delle condotte in violazione dei diritti d'autore e diritti connessi*, in *Dir. Internet*, n. 3/2008, 280.

[57] Scholars have been criticizing this approach for years now. Critics can be found in many contribution; for a specific article on the issue see C. BLENGINO, *La tutela penale del* copyright *digitale: un'onda confuse e asincrona*, in AA. VV., Copyright *digitale. L'impatto delle nuove tecnologie tra economia e diritto*, Torino, 2009, 69. For an analysis of the criminal laws protecting copyright in Italy, and a comparison with the American system, see R. FLOR, *Tutela penale ed autotutela tecnologica dei diritti d'autore nell'epoca di internet. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010.

[58] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, gave a clear account of the situation of privacy in Italy, with special reference to the introduction of computers and their increasingly massive use. He sketched some possible solutions to the already existing problems, such as the issue of control of personal information.

Some rules protecting privacy in a wide sense have been there since the introduction of L. 633/41 on *diritto d'autore*. In particular, art. 10 protects the use of a person's image; arts. 93, 96 and 97 concern the secrecy of correspondence and the rights related to portrays. With time passing, more rules were introduced in the system, such, for example, those concerning the privacy of workers by L. 20.5.1970, n. 300[59]. In 1950, Italy signed the *European Convention for the Protection of Human Rights and Fundamental Freedoms*, whose art. 8 proclaims the "Right to respect for private and family life".

Criminal provisions have been protecting people's domicile (arts. 614 and 615 cp)[60] since the enactment of the criminal code in 1930. Moreover, art. 615*bis* was introduced in 1974 to protect people's private lives from illicit interferences. The provision, which has been applied rarely[61], punishes with imprisonment those who make videos or registrations of private life's moments taking place in private residences. The same punishment is applied to those who reveal or diffuse, with any means of public information, news or images obtained in that way.

As said, a fundamental role in the emergence of a protection for the right to privacy has been played by the *Corte di Cassazione*. The Italian Supreme Court has indeed created a system of protection for privacy, drawing principles directly from the Constitution[62]. The efforts made by the Supreme Court have nevertheless been criticized for being only apparent[63].

---

[59] This statute is called "*Statuto dei lavoratori*", meaning "Charter of workers' rights". According to S. RODOTÀ, *Repertorio di fine secolo*, Roma-Bari, 1999, 205, this is the first real acknowledgment of the right to privacy in the Italian system. For an account of the sources of law which could protect privacy in the Seventies see IDEM, *Elaboratori elettronici e controllo sociale*, cit., 56 ff.

[60] "Cp" stands for "Codice Penale", which is the main source of criminal provisions in Italy. It was enacted with R.D. 19.10.1930, n. 1398.

[61] R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in R. PARDOLESI (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, Milano, 2003, 17, fn. 33.

[62] Cf. M. ATELLI, *Riservatezza (diritto alla). III) Diritto Costituzionale*, in *Enc. Giur. Treccani*, vol. XXVII, Roma, 1995, 2 ff. For an explanation of the history or privacy in the Italian system, both in scholarly works and in case law, and for further bibliography on this issue, see S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, 37 ff. For a quick overview of the many Constitutional provisions relating privacy see BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, cit., 81-90.

[63] PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, cit., 22-23.

The path followed by the Supreme Court to reach the protection of privacy started with a decision taken in 1956[64]. This case, as those that will be right after summarized, concerns the diffusion of information related to private lives of famous people. In the case decided in 1956 the question regarded two movies on the life of a famous tenor, Enrico Caruso. Both the movies told the life of the artist, and showed some awkward moments of his life, among which, for example, his attempted suicide[65]. His heirs thought that these films could damage the tenor's privacy. The *Corte di Cassazione*, however, held that in the Italian system there was no right to privacy. There were only other "rights of personality", which were singularly recognized and protected[66]. The communication to the public of information on the life of other people was considered licit, especially in those cases where the information had been obtained with licit means.

In 1963 another similar case took place[67]. A book on the life of Claretta Petacci, Benito Mussolini's mistress, had been published. Petacci's heirs sued the author of the book, since they felt that he had written information that violated the woman's privacy, damaging her reputation. The Court of Appeal of Milan recognized the existence of a right to privacy for this case, and held that this right meant the juridical power to exclude any interference coming from the extern of a person's intimate and familiar sphere[68]. The Supreme Court, however, held that there was no right to privacy. Nevertheless, the conduct of the author had violated

[64] Cass. civ., 22.12.1956, n. 4487 in *Foro it*., 1957, I, 423.
[65] Cf. PASCUZZI, *Il diritto dell'era digitale*, cit., 48. See also G. GARDINI, *Le regole dell'informazione. Principi giuridici, strumenti, casi*, Milano, 2005, 216 ff.
[66] Rights of personality ("*diritti della personalità*") are a category of rights including inalienable rights, which cannot be waived; they are part of the category of fundamental rights and freedoms, but are not confined to them. Privacy and personal data protection are included in this category (this is the reason why sometimes the data subject's consent is not enough for the processing of data; cf. S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. critica dir. privato*, n. 4/97, 599). Scholars have questioned themselves on this category for a long time, investigating whether there is a single right, or there is more than one right to personality. For this reason, academic contributions on this issue are an indefinite number. For an analysis of the entire category and for further bibliography, see P. RESCIGNO, *Personalità (diritti della)*, in *Enc. giur. Treccani*, XXIII, Roma, 1990; V. ZENO-ZENCOVICH, *Personalità (diritti della)*, in *Digesto disc. priv.*, *sez. civile*, XIII, Torino, 1995, 430. The phrases "personality rights" or "rights of personhood" does not have an equivalent in common law systems. Actually, these rights are usually included in the concept of privacy and their protection under the categories of torts and defamation. Cf. G. RESTA, *Diritti della personalità: problemi e prospettive*, in *Dir. inf. e informatica*, n. 6/2007, 1044 (see the same work for a closer and more recent analysis).
[67] Cass. civ., 20.4.1963, n. 990, in Giust. civ., 1963, I, 1280 and in *Foro it*., 1963, I, 1298.
[68] Cf. GARDINI, *Le regole dell'informazione. Principi giuridici, strumenti, casi*, cit., 217, citing the sentence of the Court of Appeal of Milan of 26.8.1960, in *Foro it.*, 1955, I, 386.

Petacci's "absolute right to personality", meaning a right to the self-determination of the individual. The protection of this right, which had *erga omnes* validity, was a limit to the publication of news pertaining private lives, unless the nature of the activity made by the person or of the communicated fact were of public interest.

Finally, in 1975, the *Corte di Cassazione* affirmed the existence of the right to privacy[69]. The situation was somehow close to what had occurred to Mister Warren one hundred years earlier. The case is usually known as the "Soraya case". Soraya Esfandiari had one time been the empress of Persia; she had then been disowned by her husband, and exiled in Italy. While having intimate behaviors with a man inside the walls of her house, she was caught by a photographer with zooming lenses. The pictures were later published in a tabloid. The former empress sued the tabloid, claiming that her right to privacy had been violated. The Supreme Court held that the Italian system acknowledge a right to privacy. This right protected those strictly personal and familiar situations or happenings which, even if occurred outside one's domicile, do not generate a socially valuable interest. These moments shall be protected against interferences that, even if licit and with no offense for honor, reputation or decency, are not justified by a public interest. The Court also held that this right would not need a precise definition: such a defintion would indeed harden the concept itself and make it less adaptable to changing times.

To reach this result, the Court leaned on a number of different provisions, coming from different branches of law. Just to give some examples, the judges considered the provisions related to the protection of the integrity of the body (art. 5 c.c.), of the name (arts. 6-9 c.c.), of the image (art. 10 c.c.). They also considered some rules related to anonymity and unpublished works (arts. 21 and 24, L. 633/41), to the protection of domicile (art. 614 c.p.), and of correspondence (art. 616 c.p.).

Furthermore, the Supreme Court extrapolated some important principles directly from the Constitution. Art. 2 states that the Italian Republic recognizes and grants inviolable human rights, as well as acknowledges the protection of human personality, both as a single person and as part of social groups within which an individual's personality can develop. Privacy was therefore to be included within these rights. Art. 3 concerns equal social dignity of people. The Court held that, in

[69] Cass. civ., 27.5.1975, n. 2129 in *Foro it*., 1976, I, 2895. As seen for the "Petacci case", lower courts had already recognized this right for years. Cf. PASCUZZI, *Il diritto dell'era digitale*, cit., 49.

order to obtain such dignity, people need to have their own space for autonomy and not to be subject to undue interferences. At this regard also art. 13, on the sanctity of personal freedom, was to be taken into consideration, article that was to be interpreted as a wider concept than the one referring simply to physical freedom. In addition, art. 14 protects the domicile against inspections, searches, and so on, while art. 15 provides for the protection of freedom and secrecy of correspondence[70].

In 1985 the *Corte di Cassazione* decided another important case[71]. Even if this decision did not concentrate primarily on privacy, it was nevertheless considered as being fundamental for the concept of information privacy: indeed, it has been considered as a solid base on which the protection of personality could be based[72]. Prof. Umberto Veronesi, a famous oncologist, had released to a newspaper an interview on the harmfulness of cigarettes with regard to cancer. The interview, which was published in 1978, contained a sentence in which the oncologist claimed that, despite new cigarettes had been created which were lighter and less harmful, these cigarettes did not eliminate the danger of cancer. Some days after the publication, the advertisement of a brand of cigarettes appeared in another newspaper. The slogan said something like: "According to Prof. Umberto Veronesi, director of the Cancer Institute of Milan, this type of cigarettes reduces the risk of cancer of almost 50%". Since this sentence was damaging prof. Veronesi's reputation, as well as that of his institute, whose aim is fighting cancer, they sued the cigarette producer and the editor of the newspaper, asking for compensation. The Supreme Court granted the request of the oncologist and held that in the Italian system there is a right to "personal identity". More precisely, there is the right of a person not to undergo misrepresentations of her own personal intellectual, political, social, religious, scientific, ideological, or professional beliefs or belongings. In other word, it is the right of a person to be represented in her real identity, as this identity is known in society[73]. This right can be traced back to art. 2 of the Constitution.

[70] The *Corte di cassazione* made reference to many other provisions; I put here those which I consider the most meaningful.
[71] Cass. civ., 22.6.1985, n. 3769, in *Foro it*., 1985, I, 2211, with commentary by R. PARDOLESI.
[72] Cf. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, cit., 23.
[73] It is probably close to the "tort of false light".

At the end of a long path, the Supreme Court had finally recognized the existence and the need for protection of the right to privacy. Nonetheless, this right was at that time only a "right to be let alone" and was still far to be considered as the right to have the control of one's own personal data[74]. The *Cassazione*'s definition was somewhat a static one, which did not consider the continuous requests of information by private or public entities to which people are subject. For this reason the mentioned idea of privacy as a "right to be let alone" could not be satisfying anymore. Hence, the attention shifted to some "dynamic profiles" and, in particular, to those usually linked to information privacy, namely the control of personal information[75].

The first legislation for the protection of physical as well as information privacy came only in 1996, again as a response of a European directive. Despite many European countries had adopted national legislations on privacy[76], the first clear intervention on this issue is Directive 46/95/EC. The OCSE, with its guidelines, and of the Council of Europe had an important influence on the way Europe arrived to the enactment of this directive[77]. Two important resolutions by the Council of Europe were incorporated in the Strasbourg Convention n. 108 of 1981, for the Protection of Individuals with regard to Automatic Processing of Personal Data[78]. In the elaboration of a comprehensive regulation for privacy, Europe considered the necessity to protect this right from electronic processing, as well as in situations

[74] PASCUZZI, *Il diritto dell'era digitale*, cit., 50.
[75] BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, cit., 101. With reference to these changes on the concept of privacy, an interesting classification was offered by a prominent Italian scholar. His idea is that persons' private sphere has been characterized by four tendencies: first, as already said, it went from the right to be let alone, to the right to control one's own information; second, from privacy to the right to informational self-determination; third, from privacy to non-discrimination; fourth and last, from secrecy to control. Cf. RODOTÀ, *Repertorio di fine secolo*, cit., 209-210. The author summarizes the path taken by privacy, for which see also *Ibidem*, 216-217.
[76] The first law was enacted in two Germany's *Länders* in 1970. Cf. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, cit., 32.
[77] The Council of Europe adopted two resolutions: the first in 1973, concerning private databases, and the second in 1974 with reference to public databases; cf. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, cit., 33.
[78] The convention, signed on 28.1.1981 by the Member States of the Council of Europe, is available at the url: http://conventions.coe.int/Treaty/en/Treaties/html/108.htm. In Italy the Convention was ratified with L. 21.2.1989, n. 98. For the history of the documents and agreements which led to the Convention, as well as for an account of the contents and of the consequences of the Convention, see BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, cit., 3 -71.

related to more classic analog archives[79]. On October 24, 1995, Europe adopted Directive 46/95/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The directive stated that "in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States"[80]. This was a vital objective for the internal market; in fact with "the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy"[81]. Most important was the directive's goal of protecting fundamental rights and freedoms, especially with regard to the right to privacy, as recognized by the general principle of Community law, as well as by art. 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms*[82]. According to recital n. 12, this protection should have been granted to "all processing of personal data by any person whose activities [were] governed by Community law", therefore excluding private use of personal data.

Italy implemented this Directive through L. 31.12.1996, n. 675[83], eventually bringing privacy regulation in the Italian system. In fact, despite already in the Eighties there had been some propulsion for the adoption of a regulation for privacy

[79] PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, cit., 34. Cf. recital n. 27, Directive 46/95/EC.
[80] Recital n. 8, Directive 46/95/EC.
[81] Citation from recital n. 9, Directive 46/95/EC.
[82] Cf. recital n. 10, Directive 46/95/EC. Despite the project of a European Constitution has never been enacted, it is worth citing its art. I-51, which text was the following: "Protection of personal data. 1. Everyone has the right to the protection of personal data concerning him or her. 2. European laws or framework laws shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities".
[83] In this work I will recall just some principles of this law, since it has been repealed by art. 183, d.lgs. 30.6.2003, n. 196, introducing the so called "Privacy Code". For a deep analysis of L. 675/96 and for further bibliography, see BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, cit.; E. GIANNANTONIO, M.G. LOSANO, V. ZENO ZENCOVICH (eds.), *La tutela dei dati personali. Commentario alla L. 675/1996*, Padova, 1999; R. PARDOLESI (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, Milano, 2003.

protection, the legislator never went beyond the drafting of bills[84]. The Italian implementation differed from the European directive in two small but significant points: first, L. 675/96 considered among the principles to be protected also natural persons' dignity; second, it placed the protection of personal identity side by side to the protection of privacy, given both these aspects the same consideration[85].

The statute was modified several times and finally repealed in 2003[86], with the introduction of what is usually called *Codice della privacy*. The law was applicable to every person processing personal data inside the Italian territory[87]. With the words "every person" the law meant to be applicable both to the private and to the public sector. This has to be seen as an expression of the global approach to the protection of personal data; approach which is nonetheless undermined by many exceptions[88].

L. 675/96 was applicable, as required by the Directive, both to automatic and to manual processing[89]. In fact, art. 1, co. 2, letter b) provided for the definition of *trattamento*, meaning "processing" of data. It has to be considered as processing every operation or set of operations, done with or without the aim of electronic or anyway automated means, relating the collection, registration, organization, storage, elaboration, modification, selection, drawing, comparison, use, interconnection,

[84] For some details on these bills see PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, cit., 40-41; NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, cit., 109-110; BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, cit., 110-121.

[85] RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, cit., 583-584.

[86] This *legge* was modified by d.lgs. 9.5.1997, n. 123; 28.7.1997, n. 255; 8.5.1998, n. 135; 13.5.1998, n. 171, 6.11.1998, n. 389; 26.2.1999, n. 51; 11.5.1999, n. 135; 30.7.1999, n. 281; 30.7.1999, n. 282; 28.12.2001, n. 467.

[87] With art. 1, co., 2, d.lgs. 28.12.2001, n. 467 the applicability of the statute was extended to the processing of personal data made by anyone on the territory of a country not party to the European Union, when this person processes the data with means situated inside the Italian territory, even if these means are not electronic or automated, except when they are used for the sole transit of the data inside the territory of the European Union.

[88] A part from specific exemptions related, for example, to journalism (art. 25) or to scientific research (art. 12, letter d), art. 4 provides for a special regime for the processing made with regard to public scopes, such as the processing made by the criminal records office (*Casellario giudiziale*). Cf. A. GIANNACCARI, *L'ambito di applicazione della legge, l'importazione e l'esportazione dei dati personali*, in R. PARDOLESI (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, cit., 165.

[89] For an explanation see GIANNACCARI, *L'ambito di applicazione della legge, l'importazione e l'esportazione dei dati personali*, cit., 142 ff. See also, P. CERINA, *Art. 2. Ambito di applicazione*, in E. GIANNANTONIO, M.G. LOSANO, V. ZENO ZENCOVICH (eds.), *La tutela dei dati personali. Commentario alla L. 675/1996*, cit., 21 ff.

blocking, diffusion, erasure or destruction of data[90]. The same article also supplied the interpreters with the definition of "personal data" (letter c). L. 675/96 considered a personal data any information relating to a natural or legal person, body or association, identified or identifiable, also indirectly, by reference to any other information, including an identification number[91].

Art. 1, co. 1, stated that L. 675/96 granted that the processing of personal data be complying with rights and fundamental freedoms, as well with the dignity of natural persons, with particular reference to the right to privacy and to personal identity. This text finally confirmed the existence of the right to personal identity, which, as seen, it was earlier only a case-law creation. This is related to the increasing awareness that identity can be harmed not only by misrepresentations by mass-media, but also when the stream of information regarding a person is handled without transparency or outside the required warranties. In the digital environment, the possibility to process fragmented data multiplies the hypothesis in which a person is partially or prejudicially represented: the person would only be the sum of her electronic information[92].

A specific discipline was introduced for some special categories of data, the most important of which are probably "sensitive data". Art. 22 included in this classification those data which are suitable to reveal racial or ethnic origin; religious,

[90] Art. 2, letter b) of Directive 45/96 provided: "'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

[91] Art. 2, letter a) of Directive 46/95 stated: "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". For an explanation of the different types of data processing, a see L. LAMBO, *La disciplina sul trattamento dei dati personali: profili esegetici e comparatistici delle definizioni*, in R. PARDOLESI (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, cit., 74 ff.

[92] See G. RESTA, *Identità personale e identità digitale*, in *Dir. inf. e informatica*, n. 3/2007, 522. The unity of a person can be easily fragmented in the virtual environment. Identity means a complete and whole representation of a person. In databases, people are often described and considered only for a special scope, givine therefore a distorted vision of the person, which is represented, for example, in compliance only with her consumption preferences. Unlike what it used to happen in the analog world, these distorted representations are not the output of a manipulation or of a mutilation of the context. They simply are a fragmented repressentazion of a complex individuality. To serve this scope cancellation, modification or block of processing are some of the possibility to be considered. Identity is in fact something which continually modifies itself. See RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, cit., 605-607.

philosophical or other kind of beliefs; political opinions; the joining to political parties, labor unions, or to organization with religious, philosophical, political or union aims. The category also included personal data suitable to reveal health status and sexual life. The idea behind the creation of a specific category for these data is the fact that they can easily lead to discrimination. In fact, all these data can be processed only with the consent of the data subject, and with the previous authorization of the Privacy Authority[93].

This latter definition leads us to introducing two extremely important aspects of the Italian privacy regulation: the data subject's consent and the role of the Privacy Authority.

Art. 11 regulated consent. In fact, the processing of personal data by private people or public entities was allowed only with the explicit consent of the data subject. Consent could be given on the entire processing or for one or more parts of it. Furthermore, consent was valid only when given freely, specifically, and in writing, and only if some particular information had been previously given to the subject[94]. Consent should be seen as a way for the individual to exercise her right to personal identity. Whenever a person denies her consent, she decides to keep her identity secret. On the contrary, whenever a person gives her consent, she decides to move from a secret identity to a "controlled" identity[95]. Art. 12 listed the cases in

[93] Cf. art. 8 of Directive 46/95/EC on "The processing of special categories of data". A part from sensitive data it should be underlined that in no cases there is neither a total absence of protection or an absolute impossibility to process an information. This means that no data is subject to an absolut publicity, since also for the most known data there is the possibility for the data subject to oppose to the processing for legitimate reasons, cf. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, cit., 591-592.

[94] The pieces of information to be given were listed in art. 10, L. 675/96: the aim and the methods of the processing; the compulsory or optional nature of data conferring; the consequences of an eventual deny to confer; the subject or category of subjects to whom the data can be communicated, and the space of diffusion of the same; the subject's rights included in art. 13, among which are the right to ask the cancellation, the modification and the update of the data. For an overview of the problems relating to consent, see S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civile*, n. 4/99, II, 455; NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, cit., 150 ff. The real efficacy of the consent expressed by the data subject was question already by RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit., 45 ff., who talks of "the myth of consent".

[95] Cf. A. FICI, E. PELLECCHIA, *Il consenso al trattamento*, in R. PARDOLESI (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, cit., 499. Consent is the most complete expression of the right to control one's own personal data, that left a person's privacy sphere; cf. G. COMANDÈ, *Artt. 11 e 12 (Consenso – Casi di esclusione del consenso)*, in E. GIANNANTONIO, M.G. LOSANO, V. ZENO ZENCOVICH (eds.), *La tutela dei dati personali. Commentario alla L. 675/1996*, cit. 133; BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, cit., 489 ff.

which consent was not needed. Just to give some examples, consent was not required when the processing and storage of data was due to a provision of a statute, a regulation or a Community law; when data were used only for aims of scientific or statistic research, if done in compliance with deontological codes; when data was necessary for saving life or safety of data subject or of a third person, for the case in which the data subject could not give her consent for a physical impairment or for legal incapability[96].

L. 675/96 introduced a privacy authority, whose first denomination was *Garante per la tutela delle persona e di altri soggetti rispetto al trattamento dei dati personali*, later modified into *Garante per la protezione dei dati personali* (commonly called *Garante della privacy*)[97]. Art. 30 stated that the authority operates with plain autonomy, as well as with judicial and evaluation independence. The *Garante* is a collective body composed by four members, elected by the two branches of the Parliament, who are presided by a president. Art. 31 described what the Authority's tasks and prerogatives are. For example, the provision requested the creation of a general register of the processing of data, based on the notification received by the *Garante*. This should allow everyone to know which data were collected in each database, increasing the transparency of the processing and storage of data, so that people could know what personal data were concerned. No databases could be created without a previous registration by the Authority, with the result that, without this registration, the database would be illegitimate. The Privacy Authority had also the duty to control if data processing is made in compliance with norms. Furthermore, it receives reports and complaints from single persons as well as from associations, and it can apply the measures considered suitable for the situation. For example, the *Garante* can inhibit illicit behavior, even if it cannot apply sanctions. Furthermore, the Authority has been assigned an important role connected to its jurisdictional powers. Indeed, under art. 29 the data subject can enforce her rights by

[96] Cf. art. 12, letters a), d), g), L. 675/96.

[97] For a commentary on this authority, its origins, and on the different ways in which this institution has been implemented in the European Countries, see R. D'ORAZIO, *Art. 30. Istituzione del Garante*, in E. GIANNANTONIO, M.G. LOSANO, V. ZENO ZENCOVICH (eds.), *La tutela dei dati personali. Commentario alla L. 675/1996*, Padova, 1999, 397 ff.

asking the intervention either of the judicial authorities or of the *Garante della privacy*[98].

With the scope of increasing citizens' awareness of privacy regulation, the Authority had the particular duty to encourage the adoption of deontological codes, of which it has to ascertain the accordance with the law. Furthermore, the Authority should take care of the knowledge of citizens on the rules relating to privacy, and of their aims[99].

In 1997 Europe enacted another directive, concerning "the processing of personal data and the protection of privacy in the telecommunications sector" (97/66/EC). The directive was enacted with d.lgs. 13.5.1998, n. 171, which modified L. 675/96, also with reference to the issue of journalism and personal data[100]. Art. 1 of the Directive specifies that the same was enacted to harmonise the provisions of Member States for the protection of personal data in the sector of telecommunications, and for these aims it was to be intended as a complement to Directive 95/46. Telecommunications services were defined as services whose provision consists totally or partially in the transmission or forwarding of signals on telecommunication networks. Interactive services were also included, even if related to audiovisual products, except for the diffusion of radio or television broadcasting (art. 1, letter d), d.lgs. 171/98)[101]. Natural and legal persons receive the protection of this directive as "subscribers" or "users" of telecommunication services[102].

The regulation introduced with d.lgs. 171/98 concerned the "dynamic moment", meaning the circulation of data through a network or a telecommunication service. On the contrary, when data were stored into a database or were subject to processing, L. 675/96 applied. Particular provisions were contemplated for data

[98] For a commentary of this function of the Privacy Authority and for further bibliography on this issue, see M. GRANIERI, *Il sistema della tutela diritti nella legge 675/1996*, in R. PARDOLESI (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 2, Milano, 2003, 437 ff; BUTTARELLI, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, cit., 463 ff.

[99] Cf. art. 31, letters h) and i).

[100] S. SICA, *Sicurezza e riservatezza nelle telecomunicazioni: il d.lgs. n. 171/98 nel "sistema" della protezione dei dati personali*, in *Dir. informazione e informatica*, n. 4-5/1998, 776. Cf. art 12, d.lgs. 171/98.

[101] See the definition contained in art. 2, letter d), Directive 97/66: "'telecommunications service' shall mean services whose provision consists wholly or partly in the transmission and routing of signals on telecommunications networks, with the exception of radio- and television broadcasting".

[102] A user differs from a subscriber, since the former does not buy a subscription, cf. P. PALLARO, *La privacy nel settore delle telecomunicazioni: la direttiva comunitaria n. 97/66*, in *Riv. dir. europeo*, n. 3/1998, 545. See the same work for a brief comment on the entire directive.

related to calls traffic: these data should have been cancelled or anonymized at the end of the call, except if needed for invoicing reasons. Nevertheless, also in this latter case, data should be cancelled after the period needed for eventual complains on invoices or on payments[103].

The regulation illustrated above was repealed and substituted by Directive 58/2002/EC. This important regulation, enacted on the 12th of July 2002, concerns "the processing of personal data and the protection of privacy in the electronic communications sector" (so called "Directive on privacy and electronic communications")[104]. To implement this directive, Italy repealed L. 675/96 and created an organic body of laws, under the name of *Codice in materia di protezione dei dati personali*[105], enacted with d.lgs. 30.6.2003, n. 196[106]. This code represents an attempt to give a unique and complete regulation for the matter of privacy.

Art. 1 proclaims that "everyone has a right to the protection of the personal data concerning him or her", using the same wording of art. 8 of the European Convention for Human Rights. The code grants that the processing of personal data is done in obedience to fundamental rights and freedoms, as well as in respect of the subject's dignity, with particular reference to *privacy, personal identity, and the right to personal data protection*[107]. With these words, eventually the legislator explicitly celebrates the existence of those rights[108]. The reference to a right to

[103] Cf. arts. 4 ff, d.lgs. 171/98.
[104] Even if it is not of importance for this research, and therefore it will not be summarized, it is worth mentioning the existence of Regulation (EC) n. 45/2001 of the European Parliament and of the Council of 18 December 2000, on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
[105] "Code on the topic of personal data protection", often called *Codice della privacy*.
[106] For a deep analysis of this legislation and for further bibliography see F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (eds.), *Il codice dei dati personali: temi e problemi*, Milano, 2004; J. MONDUCCI, G. SARTOR (eds.), *Il codice in materia di protezione dei dati personali*, Padova, 2004; C.M. BIANCA, F.D. BUSNELLI (eds.), *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, Padova, 2007.
[107] Cf. art. 2, d.lgs. 196/03. Emphasis added.
[108] According to S. NIGER, *Il diritto alla protezione dei dati personali*, in MONDUCCI, SARTOR (eds.), *Il codice in materia di protezione dei dati personali*, cit., 7, the right to data protection is a different kind of right, if compared to the traditional rights of personality. In fact, it seems that this right concerns something which is external to the person, while other rights to personality concern directly *the* person [emphasis added]. For a deeper analysis, I shall make reference to the already cited works on the rights of personality (see supra note n. 936) and to G. RESTA, *Il diritto alla protezione dei dati personali*, in CARDARELLI, SICA, ZENO-ZENCOVICH (eds.), *Il codice dei dati personali: temi e problemi*, cit., 23 ff. The right to personal data protection is now added to fundamental rights and freedoms according to S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla* privacy, in *Europa e Dir. Privato*, n. 1/2004, 3.

personal data protection is an absolute novelty compared to the text of L. 675/96, which, even if it seems merely declamatory, it actually implements a constitutional protection and gives a key to interpret the entire Code[109].

The Code is divided in three parts: the first contains general duties and rights, with reference both to private and public sectors; the second concerns specific areas where data are processed, such as the use of data by the police, by insurance companies or by banks, in the health sector, in journalism, and so on; the third part provides for the administrative and jurisdictional protection, it establishes the penalties applicable for the violation of the Code, and it also regulates the Privacy Authority bureau.

As it was already the case in the previous regulation, the Privacy Code is applicable to all the processing made by those who are established inside the Italian territory, as well as the processing made by those who are established on the territory of a non-member State, when processing the data with means situated inside the Italian territory[110]. The legislation is applicable both to private and public entities, but there are some provisions which apply only to one or the other of them[111].

Art. 4 gives a long list of definitions, which in part are those already existing in L. 675/96. For what "processing" is concerned, letter a) of art. 1 considers many different operations, which can be grouped in four distinct phases of the elaboration of personal data:

1. the preliminary phase of collection and registration of data;

[109] Cf. RESTA, *Il diritto alla protezione dei dati personali*, cit., 14. The Author starts with a critical approach, trying to understand whether art. 1 of the Code really brought something new into the Italian systems. Through an analysis of the European scenario the Author reaches the conclusion that the provision is not just a declamatory one, rather it adds a new right to the list of the rights recognized by the constitution; see *Ibidem*, spec. 41-42. This right has been considered also as a precondition for the full enjoyment of the other fundamental rights, cf. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla* privacy, cit., 4. The same Author also considers privacy as a precondition for the enjoynment of many benefits brought by science and technology, such as those related to health; cf. S. RODOTÀ, *Diritto, scienza, tecnologia: modelli e scelte di regolamentazione*, in *Riv. critica dir. privato*, n. 3/2004, 368.

[110] Even if these means are not electronic or automated, except when they are used for the sole transit of the data inside the territory of the European Union, cf. art. 5, d.lgs. 196/03.

[111] Arts. 18-22 apply only to public entities; arts. 23-27 apply to private entities and public companies.

2. the phase of use, within which organization, examination[112], elaboration, modification, selection, extraction, comparison and interconnection of data are situated;
3. the phase of circulation, including communication ad diffusion of data;
4. the terminal phase, which includes conservation, block, erasure, and destruction of data[113].

Each of these operations is defined by art. 4, which also provides for the fundamental definition of "personal data": such definition does not differ deeply from the one included in L. 675/96. In fact, the current definition comprises any information concerning a natural person, identified or identifiable, also indirectly, through reference made to any other information, including a number of personal identification. Unlike what happened in its original version, due to a recent amendment, today's wording of this definition does not comprise "legal persons" as data subject anymore[114].

The same article provides also for the definition of sensitive data, in the same formulation as already seen for the previous legislation, and for the definition of "identifying data", which are those data allowing the direct identification of the data subject[115]. Each data can be considered "anonym" when, since its origin or after the processing, it cannot be associated to an identified or identifiable subject[116].

Data subject's rights are fundamentally the same already recognized by L. 675/96. Art. 7, d.lgs. 196/03 does indeed recognize for the data subject the right to

[112] This kind of action was not considered in L. 675/96, cf. NIGER, *Il diritto alla protezione dei dati personali*, cit., 13.
[113] I borrow this classification from PASCUZZI, *Il diritto dell'era digitale*, cit., 55.
[114] The current wording of art. 4, letter b), d.lgs. 196/03 is the result of the amendments introduced by art. 40, co. 2, letter a), d.l. 6.12.2011, n. 201, which consolidated version is L. 22.12.2011, n. 214. Right after the introduction of this amendment, there have been critics related to the possibility that natural persons' data could be disclose as being part of legal persons' ones, cf. D. D'AGOSTINI, *Nessuna privacy per le persone giuridiche: le modifiche introdotte dal decreto "Salva Italia"*, CINDI – Centro innovazione e diritto, December 12, 2011, available at: http://associazionecindi.wordpress.com/2011/12/12/nessuna-privacy-per-le-persone-fisiche-le-modifiche-introdotte-dal-decreto-salva-italia/.
[115] Cf. art. 4, letters d) and c), d.lgs. 196/03, respectively.
[116] Cf. art. 4, letter n), d.lgs. 196/03. A recommendation of the European Council stated that data cannot be considered identifiable when identification requires and unreasonable amount of time and manpower, cf. Council Recommendation (EC) R97/5, February 13, 1997, on the protection of medical data. For a brief but complete account on the issue of anonymity in Italian law, see G. FINOCCHIARO, *Anonymity and the law in Italy*, in KERR, STEEVES, LUCOCK (eds.), *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, cit., 523.

know the origin of the data, the scope and methods of the processing, the identifying data of those responsible for the processing. The data subject has also the right to access her data, to obtain the modification and update of incomplete or obsolete information; she has the right to have the data cancelled when they are not needed in relation to the aims for which they had been collected (so called "right to oblivion"). Lastly, the individual has also the right to oppose to the processing of data, for example against "spamming".

Mirroring to some extent the data subject's rights, art. 11 prescribes in which way the data has to be handled. They have to be processed lawfully and with fairness; they need to be collected and registered for specific, explicit and legitimate aims, and used only in other processing operations compatible with those aims; they have to be correct and, when necessary, updated. The data also need to be pertinent, complete and not exceeding the scope for which they were collected or processed. Finally, they have to be stored in such a manner that allows the identification of the data subject, for a period of time no longer than needed for the scopes for which they had been collected or processed.

Furthermore, under art. 11, co. 2, those data which have been processed without complying with the discipline on personal data protection cannot be used.

As already seen for the regulation introduced by L. 675/96, a central role in the protection of personal data is played by consent. Under art. 13, informed consent requires the data subject be informed of:

- the scopes and methods of processing the data;
- the compulsory or optional nature of data conferring;
- the consequences of an eventual deny to confer;
- the subject or category of subjects to whom the data can be communicated, and the space of diffusion of the same;
- the subject's rights included in art. 7, above listed;
- the identification information of the people handling the data.

In fact, the processing of personal data by private or public entities is allowed only with the explicit consent of the data subject (art. 23). Consent can be given with regard to the entire processing or only to some operations of the same. It is valid only when the information considered in art. 13 have been supplied to the

subject and when the consent is freely given and proved in writing: in addition, it must be given with regard to a specified processing that has to be clearly stated[117]. Art. 24 lists a number of cases in which consent can be omitted. The situations, which are the same already contemplated by L. 675/96, are now better specified. Furthermore, the provision clarifies that in some cases, even if some kinds of processing are licit, diffusion or communications are nevertheless banned[118].

The *Codice della privacy* substituted also d.lgs. 171/98, which had implemented Directive 97/66. The provisions which were part of that legislation are now considered under arts. 121-132. Art. 133 attributes a particular task to the Privacy Authority. The *Garante* shall encourage the creation and adoption of deontological codes by ISPs for the processing of personal data. This includes ensuring uniform criteria to give adequate information to users, as well as more awareness of which data are processed and in which way. Providers and web managers should supply these codes and information directly on their websites, so that they can be easily found; their goal is to favour transparency and fairness towards users, in line with art. 11 of the Code.

For what users' data storage is concerned, ISPs are subject to the regulation applicable to every private person, since their collection of data can be considered a "database", as defined by letter p) of art. 4[119]. Providers shall cancel or anonymize calls traffic data, when they are not necessary for the transmission of electronic communications. Art. 123 states that providers can keep these data up to six months, for invoicing or payment reasons.

Art. 132 concerns data storage for aims which differ from those considered in art. 123. In the years following the enactment of the *Codice della privacy*, Europe, as well as Italy itself, introduced some new provisions on the retention of data, with the aim of contrasting terrorism. Art. 132 has been subject to an

[117] See also art. 26 for the warranties adopted for the protection of sensitive data.

[118] Cf. for example art. 24, letters f), g), h), d.lgs. 196/03. Some authors have claimed that consent has now a different role in the processing of personal data. In particular, some scholars consider consent to be necessary only with reference to sensitive data. See the opinions reported in M.A. GARZIA, *Art. 24. Casi nei quali può essere effettuato il trattamento senza consenso*, in BIANCA, BUSNELLI (eds.), *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, cit., 559-560.

[119] According to letter p), art. 4, database is every organized group of personal data, divided in one or more units, which are placed in one or more sites. Cf. the interpretation given by S. GORINI, S. NIGER, *Privacy e comunicazioni elettroniche*, in MONDUCCI, SARTOR (eds.), *Il codice in materia di protezione dei dati personali*, cit., 498.

incredible number of amendments[120]. The current text of the articles reserves what provided by art. 123 and adds that telephonic calls data are stored by the provider for twenty-four months from the date the call occurred, for the aim of investigation and repression of crimes. Digital telecommunications data are instead to be kept for twelve months from the date the communication occurred. Unanswered calls data are kept for 30 days[121].

In 2009 Europe enacted another directive which affects personal data protection law. Directive 2009/136/EC amended Directive 2002/58 and introduced an important change related to the so called "security breach notification". According to this provision, the provider of public available communication services shall promptly notify the personal data breach to the competent authority, as well as directly to subscribers and other persons concerned. The provider should also suggest the best measure to be adopted in order to mitigate the damage[122]. Italy is expected to implement this important directive in spring 2012[123].

As for the Privacy authority, the current regulation is substantially the same of the one introduced with L. 675/96. In fact, the Authority is composed by four people, elected by the two chambers of the Parliament, among whom a President is chosen[124]. The *Garante*'s tasks are enumerated under art. 154, which envisions four different sectors: tasks concerning control; interdiction tasks; promotional tasks; tasks relating to proposals and advices[125].

The Authority's controls aim at ascertaining that the processing of data by private or public entities are made in compliance of the applicable rules. This control can be made either directly by the *Garante* or thanks to the initiative of a

[120] Just to give an example, art. 123 has been modified by d.l. 24.12.2003, n. 354, which consolidated version is L. 26.2.2004, n. 45; by d.l. 27.7.2005, n. 144, which consolidated version is L. 31.7.2005, n. 155 (introducing laws to contrast international terrorism); by L. 18.3.2008, n. 48, ratifying and executing European Convention on Cybercrime, signed in Budapest in 2001; by d.lgs. 30.5.2008, n. 109, implementing European Directive 2006/24. For a brief account of the modifications intervened see A. TOLONE, *La disciplina degli obblighi di conservazione dei dati telematici da parte dei* providers, in *Riv. informazione e informatica*, n. 6/2008, 856.
[121] Cf. art. 132, co. 1 and 1*bis*, d.lgs. 196/03.
[122] Cf. art. 2, Directive 2009/136/EC.
[123] With art. 9, L. 15.12.2011, n. 217 the Italian Parliament delegated the Government to implement this directive within three months from the coming into force of the same *legge*.
[124] Art. 153, d.lgs. 196/03 also describes the characteristics that these people need to have; for example they need to be experts in informatics or law, and they have to show independence from other powers.
[125] Cf. G. PASETTI, *Il garante per la protezione dei dati personali*, in MONDUCCI, SARTOR (eds.), *Il codice in materia di protezione dei dati personali*, cit., 516.

person who can inform the Authority through a warning or a signalling. This can start a particular process, at the end of which the *Garante* can take the suitable measures. Indeed, arts. 141-151 provide for jurisdictional power for the Authority, which can take measures at the end of a special process that takes place in front of the *Garante*[126]. The Privacy Authority can also prohibit or block the processing of data, partially or totally.

Furthermore, as already stated by L. 675/96, the *Garante della privacy* shall encourage the adoption of deontological codes of conduct. This is undoubtedly a promotional role attributed to the Authority, together with its task of assuring the public awareness of privacy regulation and protection measures. Finally, the Authority has the power to signal to the Parliament and the Government the necessity to adopt new regulation to grant privacy and data protection (art. 154, co. 1, letter f). Moreover, the Government has to consult the Authority when planning norms or acts which could affect personal data protection (art. 154, co. 4). In this way, the *Garante* can preemptively evaluate the possible conflict of the would-be norms with principles granting privacy protection.

As it can be understood in reading the previous pages, the Italian framework for data protection is based on an all-encompassing statute, applicable to all the sectors of public and private life. This *Code* includes special provisions for particular kinds of data, rules for the intervention of the Privacy Authority in the public debate on data protection, particular forms of process managed by the Authority, and many other provisions which show a particular dedication to personal data protection. As we will see in the next paragraphs, the role of the Authority has sometimes being crucial for the protection of personal information, especially in the electronic communications sector.

[126] See GRANIERI, *Il sistema della tutela diritti nella legge 675/1996*, cit., and B. CUNEGATTI, *Tutela amministrativa e giurisdizionale*, in MONDUCCI, SARTOR (eds.), *Il codice in materia di protezione dei dati personali*, cit., 487 ff.

4.3 Cases and solutions

4.3.1 The Peppermint Case

a) Decisions in favor of disclosure: August 2006

The most famous Italian case on copyright enforcement against file-sharing is known as the *Peppermint* case.

Peppermint is a German recording company which holds the copyright on many musical works of different artists. In autumn 2006, a legal firm based in Northern Italy started sending thousands of letters on behalf of Peppermint to Internet users accused of illegal file-sharing[127]. The letters claimed that, thanks to the collaboration of another company called Logistep, Peppermint was aware that the recipient of the letter had made available on her computer, and exchanged through a peer-to-peer system, sound recordings on which Peppermint hold copyrights. Logistep was a Swiss company that used a modified version of file sharing clients in order to register IP addresses, pseudonymous, and other users' data[128]. The letter informed the user that her data had been supplied by her ISP, following an order from the Tribunal of Rome[129].

The letter contained also a sort of settlement agreement: if the user had deleted immediately all the files and paid 330 € as a partial compensation for the damages, then Peppermint would have not sued the user and not notified the public authority of her illegal behaviour, which is criminally punishable[130].

---

[127] Examples of the letters sent can be found at the URL http://xp2p.altervista.org/?p=11.

[128] According to the news, the Swiss branch of the company was closed in 2010, see A. MARUCCIA, *Logistep, fine dei giochi. In Svizzera*, Punto-informatico.it, September 10, 2010, available at http://punto-informatico.it/2987767/PI/News/logistep-fine-dei-giochi-svizzera.aspx. Logistep still exists in Germany (cf. http://www.logistep-deutschland.de/).

[129] Trib. Roma, ord., 18.8.2006 in *Riv. dir. Ind.*, n. 4-5/2008, II, 328, with commentary by M. DE CATA. See also Trib. Roma, ord., 19.8.2006, in *Dir. Informatica*, n. 4-5/2007, 815 and in *Il civilista*, n. 5/2008, 30, with commentary by F. VALERINI. According to G. FOGLIA, *La* privacy *vale più del diritto d'autore: note in materia di* filesharing *e di sistemi* peer-to-peer, in *Dir. industriale*, n. 6/2007, 598, this decision was confirmed also after the appeal of Wind (Trib. Roma, ord., 22.9.2006), and the same conclusion was also reached in another lawsuit between the same parties (Trib. Roma, ord., 9.9.2007.

[130] The point is questionable: in particular, in Italy there are crimes which can be prosecuted *ex officio* by the Prosecuting Attorney (*Pubblico Ministero*), meaning without the need of any notification, and crimes which need a prior complaint from the victim of the crime. The crime in question (the one punished by the previous text of art. 171, co. 1 letter a-*bis*), L. 633/41) is indeed prosecutable *ex officio*, meaning that the promise of Peppermint to not notify the illegal behavior lacked of consistency.

The letter were sent since Peppermint had obtained users' personal data as per, as mentioned, an order of the Tribunal of Rome. In June 2006, Peppermint asked the Tribunal of Rome to order Wind Telecomunicazioni s.p.a.[131], an ISP, to disclose the data associated to its users who allegedly infringed Peppermint's copyright. Peppermint explained that many songs of which Peppermint owned the copyright had been exchanged through a peer-to-peer system. The plaintiff also claimed that many of the IP addresses registered by Logistep belonged to Wind's customers. Furthermore, Peppermint explained that, as had happened for RIAA and CRIAA, IP addresses could be linked to customers' information only by the ISP. For these reasons, the plaintiff asked the Tribunal to order Wind to disclose the data related to the alleged infringers, in compliance with art. 156*bis*, L. 633/41.

As already explained, this article provides a remedy for a party that gives serious elements of proof from which it is possible to reasonably infer the grounding of its requests and that has identified documents, information or other elements held by the counterparty. If these information or documents could confirm the elements of proof given by the plaintiff, then the latter can obtain a judicial order that disposes the exhibition of or asks for the information. The same article states that the plaintiff can obtain an order in which the judge asks the counterparty to supply the elements for the identification of the subjects who are involved in the production or distribution of the products or services which constitute violation of copyright.

The same article also provides that in these orders the judge has to adopt some suitable measures so that confidential information can be protected (art. 156*bis*, co. 3)[132]. In some interpretations, this article provides for an action to obtain a precautionary measure[133]. Precautionary measures aim at avoiding that the situation in which a right holder stays could get worse with time passing and that her rights does not undergo an irreparable prejudice. They typically provide for injunctions which enjoin the counterparty from a particular action or impose the counterparty a

[131] WIND Telecomunicazioni s.p.a. offers different services such as telephone, mobile phone and Internet, cf. http://www.windgroup.it/it/investitori/profilo.phtml.

[132] Actually, the a subsequent decision of the Tribunal of Rome stated that art. 156*bis* does not provide for a precautionary measure, rather it provides a tool for discovery. Cf. Trib. Roma, 17.3.2008, in *Giur. it*., n. 7/2008, 1738, with commentary by A. SIROTTI GAUDENZI (see later in this chapter for a summary).

[133] As said in the previous paragraph, according to some scholars art. 156*bis* introduced a tool for discovery in the Italian system. In this judgment, however, the Tribunal considered art. 156*bis* as introducing a precautionary measure. Therefore I shortly illustrate the way this measures function.

particular behaviour. This kind of actions has some peculiar characteristics. First of all, they are instrumental to a subsequent plain lawsuit. This means that they can be temporary and, therefore, cannot bring to definite solutions, since for a definite solution a plain lawsuit would be necessary. This is particularly true for the fact that these lawsuits are concise, meaning that judicial measures are taken on the base of elements of proof given by the claimant: there is no investigation for evidence. Nevertheless, there are lawsuits whose outcomes can also have effect indefinitely[134]. An injunction can be ordered by a judge when the two main requirements of the action exist: *fumus boni iuris* and *periculum in mora*. The latter is the risk of an imminent and irreparable damage. The former is the presumption of sufficient legal basis in order to grant the requested measure[135], with a precognition of what will be the result of the entire lawsuit[136].

Some authors claim that *periculum in mora* is *in re ipsa* in the case of violation of economic copyrights. This would mean that, since it is sure that the damage would worsen during the time of the lawsuit, there is no need to prove it. Nevertheless, judges have held that this is not the case and that the existence of a danger has to be proved by the claimant in order to obtain the requested injunction[137].

Peppermint claimed that the requested data needed to be disclosed with no delay, since ISPs retain this kind of information only for six months. Moreover, the longer had been the delay, the bigger would have been the damage for Peppermint, since file-sharing gives an alternative method for obtaining the same songs that the recording industry sells.

As for the instrumentality of the requested measure, Peppermint held that this request was needed in order to later sue Wind for obtaining the exhibition of alleged infringers' data.

---

[134] Cf. C. MANDRIOLI, *Corso di diritto processuale civile*, Editio minor, vol. III, Torino, 2011, 240; C. CONSOLO, *Spiegazioni di diritto processuale civile. Vol. I. Le tutele: di merito, sommarie ed esecutive*, Torino, 2010, 269-270.

[135] MANDRIOLI, *Corso di diritto processuale civile*, cit., 238.

[136] CONSOLO, *Spiegazioni di diritto processuale civile. Vol. I. Le tutele: di merito, sommarie ed esecutive*, cit., 271. The author explains that each precautionary measure has its own charachteristics, see *Ibidem*, 272.

[137] Cf. SIROTTI GAUDENZI, *Il nuovo diritto d'autore*, cit., 368. The author nevertheless writes that many judicial decisions held that if the claimant alleges the day by day prosecution of the violation and consequent damage, then this is enough to prove the existence of *periculum in mora*.

Wind counterclaimed that the request was not admissible for many different reasons, one of which was that, in Wind's opinion, plaintiff's action was not legitimate, since Peppermint was not the actual holder of the economic rights on the alleged uploaded songs. Wind also claimed that there was no proof that the illegal alleged upload had been made by Wind's users and that, as a consequence, it should not have been Wind to act as defendant. Moreover, Wind alleged that Peppermint had collected users' data illegally, in violation of privacy law.

Wind also wrote in its counterclaim that it could not be considered as an intermediary as required by art. 156, L. 633/41 and, therefore, it could not receive such an order as the one requested by Peppermint. In fact, art. 156 provides a remedy for the case that a copyright holder fears the violation of her economic right or wants to prevent the perpetuation or repetition of an already existing violation. The copyright holder can prevent or stop the infringing activity by asking a judge either to stop the infringer or to stop the activity of an intermediary providing the services used as a mean to the infringing activity.

The defendant also claimed that the kind of order asked by Peppermint could have been issued only by a criminal law judge, due to arts. 23 and 132 of the *Codice in materia di protezione dei dati personali*. In fact, as seen, personal data can be collected only with the data subject's consent, as requested by arts. 23. Furthermore, art. 132 of the same *Codice* states that data related to telephone traffic are kept by intermediaries for thirty months for the scope of crime repression. For what it can be understood from the sentence, probably in Wind's interpretation this reference to "crime" means that only inside a criminal trial an ISP can be asked to show this kind of data.

Lastly, Wind claimed that a *periculum in mora* was totally absent. For these reasons the defendant asked for the rejection of Peppermint request.

The proceeding judge notified the Privacy Authority of the existence of the lawsuit between Peppermint and Wind, as required by art. 152 of the *Codice in materia di protezione dei dati personali*. Nonetheless, the Privacy Authority did not step in the lawsuit[138].

[138] See Trib. Roma, ord., 18.8.2006 cit., paras. 1-3.

The Tribunal considered Peppermint's request admissible. As for instrumentality, the judge claimed that it was *in re ipsa*, given that the subsequent lawsuit would have been commenced to obtain users' data, exactly as in the precautionary measures.

For what *fumus boni iuris* was concerned, the Tribunal of Rome held that, unlike what had been claimed by Wind, Peppermint had correctly and sufficiently proved to be the holder of the copyright on the songs allegedly uploaded. Peppermint had also proved that some of these songs had been made available in the web by Internet users. The Tribunal based these argumentations on a report by an expert[139]. In the judge's view, this report was accurate and gave "serious, precise and concordant"[140] elements of proof on the existence of the illegal file-sharing alleged by Peppermint. Peppermint had in fact provided 356 dossiers with users' names, uploaded files, time and date of the upload(s), IP addresses, hash codes and GUIDs[141]. Furthermore, the judge was persuaded by the description of the way in which Peppermint had obtained users' data. He geld that the collection of IP addresses had been rational, since a software which could registered IP addresses of users connected to a file-sharing system was used. The same software also organized the data through a specific database, called "MS Access 2003". In the Tribunal's opinion the way these data had been collected and processed by the company in charge (i.e. Logistep), was reliable, acceptable and also licit, since a person using a file-sharing software shows her will to accept that her IP address could be recognized by all the other users of the same system. Furthermore, the fact that softwares like e-Mule or Gnutella were, in judge's opinion, largely used for offering or obtaining songs, was well known and was therefore another element of proof for the facts alleged by Peppermint[142].

---

[139] The decision of the Tribunal of Rome talks about a report by a person named "Zimmermann", who was probably an expert, a consultant for Peppermint. Cf. Trib. Roma, ord., 18.8.2006 cit., par. 5.

[140] Art. 2729 of the Italian Civil Code provides the so called "simple presumptions" as a proof for certain specific cases. These are presumptions which are left to judges' discretion and prudence. The judge shall not admit presumption which are not "serious, precise and concordant" ("presunzioni gravi, precise e concordanti" in the original version).

[141] GUID, acronym of "Globally unique identifier". It is "[a]n identification scheme in which only one name is associated with a particular object; this name is accepted across platforms and applications". Cf. *Entry: GUID*, AA.VV., *Microsoft Computer Dictionary*, Washington, 2002.

[142] Cf. Trib. Roma, ord., 18.8.2006 cit., par. 5.1. For a critic of how the Tribunal applied art. 156*bis* in this sentence see M. DE CATA, *Il caso "Peppermint". Ulteriori riflessioni anche alla luce del caso "Promusicae"*, in *Riv. dir. industirale*, n. 4-5/2008, 411 ff.

For these reasons, that is for the reliability and accuracy of the collected data, the Tribunal held that it was clear that the users who had uploaded Peppermint's song were Wind's customers. Next step was to clarify whether a copyright holder could ask a third party to exhibit alleged infringers' data. The Tribunal held that it was possible.

In particular, the judge made a comparison between the common *actio ad exhibendum* provided by art. 210 c.p.c. and the one provided by arts. 156 and 156*bis*, L. 633/41. The former requires the person requested to exhibit the documents to be one of the parties of the process. On the contrary, the latter permits to ask also a third party for the exhibition of documents. As mentioned, art. 156, introduced by d.lgs. 140/06, provides the possibility for the copyright holder to obtain an injunction against the alleged infringer as well as against the intermediary, whose infrastructures permitted the violation. In the Tribunal's opinion an ISP supplying access to the Internet is with no doubts an intermediary as understood by art. 156, since its service permits the exchange of files through file-sharing systems.

Art. 156*bis*, then, permits the copyright holder to ask for the exhibition of "documents, elements or information" held by the other party. In particular, even if art. 156*bis* uses the word "counterparty", in the judge's view this term should be interpreted as "the person holding the needed documents", which becomes the defendant in the process *ex* art. 156*bis*[143].

Furthermore, the *Codice in materia di protezione dei dati personali* does not prevent from the just illustrated exhibition. Art. 24, co. 1, letter f) of the *Codice* holds that personal information can be processed, as long as it is not diffused, without the

[143] Cf. Trib. Roma, ord., 18.8.2006 cit., paras. 6-6.1. This provision gives problems of interpretation probably due to its less than precise implementation in the Italian system. The text of art. 8, Directive 2004/48 provides that information can be asked to the infringer or to someone who was found on a commercial scale to be providing services used for the infringement. The European provision made reference to someone who effectively contributed to the infringement, and the provider, at least in this case, cannot be considered as such. Furthermore, the liability of ISPs in the European and Italian contexts would not make liable a mere conduit provider such as Wind for this kind of activities. See C. BLENGINO, M.A. SENOR, *Il caso "Peppermint": il prevedibile contrasto tra protezione del diritto d'autore e tutela della* privacy *nelle reti* peer to-peer, in *Dir. inf. e informatica*, n. 4-5/2007, 838-839. In the opinion of another author, the provision of art. 156*bis* should be read as referred only to the parties of the lawsuit concerning the enforcement of copyright. Only those parties should produce documents and information requested, but not third parties. See G. SCORZA, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto interno*, in *Dir. Internet*, n. 5/2007, 467. This interpretation would consider art. 156*bis* as a "copy" of art. 210 cpc. On this issue see also DE CATA, *Il caso "Peppermint". Ulteriori riflessioni anche alla luce del caso "Promusicae"*, cit., 414 ff.

data subject's consent, when this is necessary for the exercise or for the defence of a right inside a process. In the Tribunal's interpretation, this was the case for the request by Peppermint. In fact, the plaintiff company had no other means to obtain the real identities of users through their IP addresses. Art. 132, mentioned by the defendant, was not pertinent to the lawsuit, since it concerns the storage and not the handling of telephone traffic data[144].

As for the requirement of *periculum in mora*, the Tribunal held that it was to be considered *in re ipsa* for two reasons. First, the impossibility for Peppermint to obtain the identities of infringers permits the latter to perpetrate the illicit conduct. The chances to access and acquire a song through a file sharing network increase with the increase of the number of users with that song stored on their computers. Therefore, the latter is the intervention against the uploader, the higher is the possibility for other users to obtain the song. As already recognized by US and Canadian judges, also the Italian judge acknowledged that this is a sort of multiplier effect[145].

The second reason for which there is a danger for the plaintiff is actually a bunch of different reasons: the dimensions of the web; the fact that the Net is beyond control; the ease with which it is possible to obtain a file-sharing software through the web. All these reasons create the serious and concrete danger of a misdirection of Peppermint's customers from the market to the file-sharing system.

Following these argumentations, the Tribunal of Rome ordered Wind to give Peppermint the following information about the alleged infringers: name, surname, address, place and date of birth or, as an alternative, the "tax code"[146].

b) February 2007

The requests of Peppermint did not stop and in the autumn of 2006 the German recording company asked again the Tribunal of Rome to order another ISP the disclosure of its customers' data. The decision taken at the end of November was

[144] Trib. Roma, ord., 18.8.2006 cit., par. 6.2.
[145] Trib. Roma, ord., 18.8.2006 cit., par. 7.
[146] The "tax code" ("*Codice Fiscale*" in Italian) is an alphanumeric code that every individual has since her birth and which is associated with her fiscal position. From a *codice fiscale* it is possible to trace back name, surname, place and date of birth of the person associated to the code.

against the disclosure[147]. Peppermint contested the order, which was revised by another section of the same Tribunal[148].

The request of Peppermint was based again on article 156*bis*, L. 633/41, and asked for the disclosure of some of the defendant's customers. According to the interpretation made by this section of the Tribunal, the mentioned article introduced a new way to protect intellectual property rights, giving the plaintiff the possibility to acquire, from the counterparty, elements and information needed as evidence to obtain a plain recover for the damages. Law had therefore provided the possibility to oblige the counterparty, who was directly or indirectly involved in the illicit conduct, to exhibit data and information related to further subjects involved in the same illicit conduct. This interpretation leads to the conclusion that only those who are somehow, even if indirectly, responsible for the violation of intellectual property rights can be subject to the order pursuant to art. 156*bis*. This explanation would also be in line with the exceptionality of this provision, which remains an invasive tool[149].

The Tribunal did not agree with the decision of the other section. The latter had interpreted art. 156*bis* term "*controparte*" (i.e. counterparty) as restricted to the actual infringer. By doing so the judge had restricted the application of the provision, so that it would not be different in any way fro, the already existing provision envisioned in art. 210 cpc. This would erase the underlying reason for the introduction of art. 156*bis*, which was to enhance the enforcement of intellectual property rights, as required by European Directive 2004/48/EC. On the contrary, in the decision summarized here the Tribunal interpreted art. 156*bis* in the light of art. 8 of the just mentioned Directive. Under letters a), b), and c) of art. 8 it should be possible to obtain information and data not only by the author of the violation, but also by someone who "a) was found in possession of the infringing goods on a commercial scale; b) was found to be using the infringing services on a commercial scale; (c) was found to be providing on a commercial scale services used in

[147] Even if not all the decisions taken by judicial organs are published in Italy and, therefore, there is no trace of the order of November 2006, according to the text of the decision Trib. Roma, ord., 9.2.2007, the contested order was taken on 28-29.11.2006 by the Tribunal of Rome. See Trib. Roma, ord., 9.2.2007, in *Resp. civ. e prev*., n. 7-8/2007, 1699, and in *Riv. dir. ind*., n. 4-5/2008, II, 328, with commentary by M. DE CATA. The decision does not mention the name of the defendants, which anyway is an ISP. For another decision ordering the disclosure see Trib. Roma, 26.4.2007, in *Riv. dir. ind*., n. 4-5/2008, II, 328, with commentary by M. DE CATA.
[148] Trib. Roma, ord., 9.2.2007, cit.
[149] Cf. Trib. Roma, ord., 9.2.2007, cit.

infringing activities"[150]. Therefore, the 156*bis*'s term *controparte* is to be interpreted as persons other than the direct infringer and to whom no violation can be attributed. It follows from these considerations that art. 156*bis* provides intellectual property rights holders with a necessary tool to understand who violates their rights, and what the concrete and real extent of the illicit conduct is. No different interpretation could be made, given that, if the term "*controparte*" referred to the alleged infringer, then the provision itself would be useless, since it would only duplicate what already provided by art. 210 cpc.

The Tribunal of Rome considered also the wording of art. 156, L. 633/41. The fact that this article considers the possibility of an injunction also towards an intermediary, such as an ISP, can be read as a confirmation of the just illustrated interpretation of art. 156*bis*.

The Tribunal then considered the argument of privacy and, in particular, the objection made by the defendant that art. 156*bis* would contrast with art. 24 of the *Codice in materia di protezione dei dati personali.* As already explained, art. 24 permits the processing of personal data without the data subject's consent, when they are needed to obtain judicial protection of someone else. The Tribunal considered, as already happened in the above illustrated decision of August 2006, that this was the case in the lawsuit between Peppermint and the ISP. This would not be in contrast with privacy legislation, given that the European Directive 2004/48/CE is subsequent to the D.lgs. 196/03 and yields the application of privacy legislation. Therefore, in the Tribunal's opinion, art. 24 is in harmony with the European legislation and, in fact, already balances information privacy protection and copyright holders' need for justice.

This interpretation would be strengthened by the existence of art. 24 of the Italian Constitution, which provides that everyone can take judicial action to protect her own rights[151]. The presence of this provision, concurs in supporting the conclusion that privacy can be sacrificed when facing someone's need for judicial protection of her rights. In the Tribunal of Rome's opinion, art. 156*bis* asks for a

[150] Letter d) of art. 8 states that the same order can be asked towards people mentioned by the subject indicated under letters a), b) and c).
[151] Art. 24, co. 1, of the Italian Constitution approximately says: "Everyone can take judicial action to protect her own individual rights and legitimate interests".

number of serious elements that the judge has to assess before ordering the disclosure of the data. The balancing is in the hand of judges, who should order the disclosure only when the case really needs to go over privacy. The request for serious elements is another index of the fact that the term "*controparte*" has to be interpreted in a wider sense. Serious elements for the disclosure would not be needed if the requested person was the infringer itself and art. 210 cpc would be sufficient. They are needed, instead, because the requested party is not the data subject.

The Tribunal also considered the collaboration that ISP should give for the enforcement of intellectual property rights, which was at the base of Directive 2000/31/EC and of the subsequent D.lgs. 70/03. In fact, the exemption from liability for ISPs introduced by this Directive, had, as a counterbalancing factor, a duty of collaboration imposed on them in the battle for intellectual property rights enforcement. This duty can be drawn from the entire structure of the Directive and it is indeed fundamental, considered that, without the collaboration of ISPs it could be not possible to understand who the infringers are.

Following this reasoning, the Tribunal granted the order to disclose every piece of information suitable for the identification of the alleged infringers, as requested by Peppermint[152].

c) Decisions against disclosure: July 2007

Heartened by the results of the first lawsuits, Peppermint went on suing ISPs to obtain users' data. Meanwhile, thanks also to the letters sent by the law firm representing the recording company, the "Peppermint case" started to become more and more famous, attracting the interest of scholars, users and consumers' associations.

In the case decided by the Tribunal of Rome in July 2007[153], plaintiffs were Peppermint and Techlands Sp. z o.o., a videogame company. As in the previous cases, Peppermint and Techlands argued that they had detected the exchange of music files and video games files through peer-to-peer systems. With the aid of

[152] So, in this case, The Tribunal did not precisely state which data should be disclose, rather it only order the disclosure of suitable information, somehow worsening the situation for users.

[153] Cf. Trib. Roma, ord., 16.7.2007 in *Dir. informatica*, n. 4-5/2007, 828, with commentary by C. BLENGINO and M.A. SENOR. See also the decision Trib. Roma, ord., 14.7.2007 in *Riv. dir. ind*., n. 4-5/2008, II, 330, with commentary by M. DE CATA.

Logistep, the two companies had obtained the IP addresses and GUID numbers of the alleged infringers, who came out to be again customers of Wind. On the basis of these findings Peppermint and Techlands sued Wind under art. *156bis*, L. 633/41 to obtain users' information. In their claim, the two companies underlined that art. 24 of the *Codice in materia di protezione dei dati personali* did not constitute an obstacle to the disclosure of data, since them were needed for the judicial protection of intellectual property rights, even if it was a civil and not a criminal trial.

In its counterclaim, Wind pointed out that the request by Peppermint and Techlands was not grounded, and, in particular, *fumus boni iuris* was missing for the following reasons:

- the communication of personal data could be ordered only within a limited period of time, in connection with specific crimes (listed in art. 407, co. 2, letter a), c.p.p.)[154] and, therefore, only when asked by the *Pubblico Ministero* (Public Prosecutor). This provision had to be considered exceptional and therefore could not be interpreted extensively for the application to similar cases[155];
- only art. 163, L. 633/41 provides the possibility for copyright holders to obtain injunctions towards ISPs, whereas articles 156 and 156*bis* do not mention ISPs. Furthermore, these latter articles require the intermediary to be involved directly or indirectly in the violation. Wind claimed that it was not involved, given that its only activity was to supply the Internet connection to users;
- art. 123 of the *Codice dei dati personali* prescribed that ISPs had to delete this kind of data or, anyway, to anonymize them[156]. This meant a juridical impossibility to disclose the requested data;

[154] *C.p.p.* stands for "*Codice di procedura penale*", the Italian criminal procedure code, D.P.R. 22.9.1988 n. 447, which came into force on the 24th October 1989. The limitation on the communication of data came from
art. 132, d.l. 27.7.2005 n. 144. It was the so called "Pisanu decree", from the name of the Minister Giuseppe Pisanu, who was the promoter and signatory of the decree. The decree, which contained urgent measures against terrorisms, was later converted into law: L. 31.7.2005, n. 155.

[155] The Italian Civil Code opens with some preliminary provisions, which are usually applied to all the branches of law. In particular, art. 14 provides a rule for interpretation of criminal laws and exceptions. Both of them cannot be apply beyond the cases and the time for which they have been introduced.

[156] The text of art. 123 is now different.

- the collected IPs and GUIDs were not usable since they had been acquired in violation of privacy law. In fact, in the phase of acquisition of these data, users should have been informed of the collection of their information and, only after been informed, they could have consented to their processing. In fact, the mentioned exemption provided by art. 24 of the *Codice dei dati personali* refers only to the judicial phase and not an eventual previous phase, such as the one in which Logistep collected users' IPs and GUIDs;
- since IPs and GUIDs are changeable, they cannot be qualified as "serious elements" as required by art. 156*bis*;
- finally, Peppermint and Techlands had not effectively proved to be the copyright holders of the allegedly infringed works.

As for *periculum in mora*, Wind claimed that, since the plaintiffs had tolerated file-sharing for long time before taking action against it, it was now contradictory to ask for a prompt disclosure of the names.

Unlike what had happened in the previous cases, this time the Privacy Authority voluntary stepped in the lawsuit and offered its remarks on the privacy issues. The Authority held that the processing of personal data related to electronic services in the "information society" was restricted to criminal judgments. In particular, it would be limited to criminal investigations made by public authorities which are in charge of national security and defence. In the Authority's opinion a different interpretation would have led to a violation of the fundamental rights of privacy and secrecy of communications, protected by the Italian Constitution, as well as by European law and by the European Convention on Human Rights. The compression of these fundamental rights could be made only when required for the safeguard of superior principles protected by criminal law. The request of Peppermint and Techlands should have been therefore rejected, since related to goods with a lower relevance than the secrecy of communications.

In order to sustain its argumentation, the Authority argued that European Directive 2002/58/EC imposed on Member States to enhance the protection and privacy of electronic communications. At the same time the Directive prohibited the storage of traffic data (including IP addresses and users' personal data), with

exception of data retained for the aim of preventing and prosecuting crimes. This exception does not comprise civil offences.

As illustrated, Directive 2004/48/EC was introduced for the enforcement of intellectual property rights. With this aim, it carried a provision imposing the disclosure of information on the origin and distribution of goods and services prejudicial to the rights to persons who are not the author of the violation. At the same time it reserved the limitations inserted in the privacy regulations. In the Authority's interpretation this construction of the Directive meant that the European legislator considered privacy to be prevailing on intellectual property enforcement.

Directive 2001/29/EC introduced the possibility for copyright holders to obtain an injunction toward a third party; but this was not possible in this specific case. Moreover, the same Directive (art.9) expressly yielded other provisions, among which was the protection of personal data.

D.lgs. 196/03, being the implementing statute of Directive 2002/58/EC, introduced the same limitation posed by the latter. The only exception for the conservation of personal data and electronic communications traffic data was the one mentioned by Wind, meaning the repression of the crimes listed in art. 407, co. 2, letter a) c.p.p., and the crimes carrying detriment to information systems. This had been confirmed also by the Italian Constitutional Court in the sentence n. 372/2006, relating to art. 132 of the *Codice della privacy*[157].

Furthermore, the collection and processing of users' data made by the plaintiffs had to be considered illicit, because violating the *Privacy Code*. In particular, Logistep's monitoring activity should have been previously authorized by the Privacy Authority as well as by the data subjects themselves, as required respectively by arts. 37 and 13 of the same *Code*. The omission of authorization meant that the collecting was illicit and, in turn, that the data could not be used for any other processing, as prescribed again by the *Code* (art. 11).

[157] The Constitutional court held that art. 132 of the *Privacy Code* was not in contrast with the Constitution. In fact, the fundamental right to privacy protection can vary according to the concrete need that privacy itself is facing, as long as this need is recognized by the Constitution. Higher or lower protection needs to be balanced with the higher or lower gravity of different crimes. This balancing appertains to the legislator. See Corte Cost., 14.11.2006, n. 372 (spec. par. 5 ff.) in *Dir. Informatica*, n. 1/2007, 133; in *Cass. Penale*, n. 3/2007, 926 with commentary by G. MELILLO; in *Giur. Cost*., n. 6/2006, 3916 with commentary by M. PINNA.

Lastly, arts. 156 and 156*bis*, L. 633/41 had to be interpreted in the light of the Constitution and, in particular, in the light of arts. 2 and 15 regarding the privacy and secrecy of communications. These fundamental rights can be restrained only when they face collective values usually transfused into criminal laws and criminal sanctions: they cannot be limited by private interests.

In the beginning of its decision, the Tribunal acknowledged that, given the new defences advanced by Wind and also given the voluntary participation of the Authority in the case, the requests of the plaintiffs had to be rejected. In fact, art. 156*bis* could be interpreted in an extensive way, so that it would comprise also the request for information held by third parties not involved in the illicit conduct. This would be in line with European Directive 2002/58/EC which, as illustrated, expressly mentions this possibility. In the previous lawsuits, the plaintiffs had obtained the disclosure of users' data exactly on the base of this provision. But this time, the Tribunal considered the argumentations to be not convincing.

Art. 156 and 156*bis* cannot be applied neither to data and information related to electronic communications nor to the traffic data produced. Indeed, the Italian and European laws on secrecy and privacy of communications among private persons provide for a prohibition related to the processing and diffusion of these data. The only exception to such ban concerns the protection of values of a higher rank than intellectual property, such as in the case of criminal laws protecting collective interests. On the contrary, the use of data related to electronic communication for the enforcement of private rights is not allowed. More precisely: according to the interpretation of the Tribunal of Rome, art. 24 of the *Codice della Privacy* allows the use of personal data without the data subject's consent also for the enforcement of private rights. But this is true only when the plaintiff already holds the information and, above all, when the information was lawfully collected.

The requests of Peppermint and Techlands concerned a different scenario. The two companies had in fact asked to obtain users' personal data, meaning that it was a phase preceding the one described by art. 24. Therefore, art. 24 could not constitute the basis upon which the plaintiffs could obtain the disclosure of the information. Furthermore, as illustrated by the Authority in his intervention, the information held by the two companies had been collected illicitly, for the lack of

authorization by the Authority and by the data subjects. For both these reasons, art. 24 could not be invoked by the plaintiffs as a justificaion to obtain the disclosure of data. Moreover, since the information had been illicitly collected, it ought not to be used for any other judicial reason, as prescribed by art. 11 of the *Privacy Code*. The information could not, therefore, be considered "serious elements" on which the judge should have ordered the disclosure as prescribed by art. 156*bis*.

Despite these argumentations constituted a sufficient ground to reject the request of Peppermint and Techlands, the Tribunal added an interesting reasoning on secrecy of communications. Actually, the Tribunal wrote that the fundamental reason to reject the plaintiffs' request was exactly the limit posed by the secrecy of communication among people, a value protected directly by arts. 2 and 15 of the Constitution. This right to secrecy could be overcome only by other interests with the same or higher constitutional relevance and, in any case, always with a balanced approach of comparison. It is exactly this approach that permits the compression of secrecy and privacy of communication when facing criminal laws protecting collective interests[158].

Even if Directive 2004/48/EC introduces a number of measures for the improvement of the enforcement of intellectual property rights, the same legislation expressly yields the protection of privacy as prescribed by the dedicated European Directives. Hence, it would be in contrast with the *IPR Enforcement Directive* to consider the disclosure of data under art. 156*bis*.

At the same time, Directive 2002/58/EC expressly prohibits the conservation of electronic communications traffic data, except under some specific circumstances that the Directive itself lists (art. 15). The Italian Constitutional Court intervened exactly on this point with the decision n. 372/06. The Constitutional judges clarified that the conservation of data for a longer period than the one required by art. 132 of the *Codice della Privacy* was legitimate given that it was needed for the balancing of privacy against collective interests.

[158] The mentioned art. 407, co. 2, letter a) c.p.p. lists serious crimes, punished with more than 5 years of jail. Among them are the organization of people with the aim of terrorism or mafia; the production and distribution of war weapons; the production and distribution of drugs, and so on.

Following all the reasoning explained so far, the Tribunal of Rome rejected the requests of Peppermint and Techlands for the impossibility to apply art 156*bis*, L. 633/41 and art. 24 of the *Privacy Code*[159].

4.3.2 The Promusicae Case

In June 2006 the *Juzgado de lo Mercantil* n. 5 of Madrid asked for a preliminary ruling by the European Court of Justice, under art. 234 of the European Community Treaty[160].

The lawsuit mirrored exactly the Peppermint cases. In the Spanish case, *Productores de Música de España* (Promusicae), a trade group, representing the Spanish recording industry, sued *Telefónica de España SAU*, a national telephone operator and ISP, to obtain alleged infringers' data. Founding himself in the same situation of the Italian judge, and not knowing how to balance users' privacy with copyright enforcement, the *Judgado de lo Mercantil* asked for the intervention of the European Court of Justice[161].

As mentioned, the Spanish case was absolutely similar to the Peppermint's. In November 2005 Promusicae had made an application to the *Juzgado de lo Mercantil* for preliminary measures against Telefónica. The plaintiff had asked the *Juzgado* to order Telefónica the disclosure of the identities and physical addresses of some of its customers, whose IP addresses were held by Promusicae. Promusicae had claimed that those individuals had used peer-to-peer systems (in particular KaZaA) to access and share phonograms of which the plaintiff itself had the exploitation rights. In other words, Promusicae had claimed before the *Juzgado* that Telefónica's customers had infringed intellectual property rights. Therefore it had sought the disclosure of their information in order to sue them in a civil proceeding.

In December 2005 the Spanish judge ordered the preliminary measure requested by Promusicae. Telefónica appealed, claiming that under the Spanish Ley

[159] It goes in the same direction also the subsequent decision of Trib. Roma, ord., 22.11.2007, in *Foro it*. 2008, 4, I, 1329 with commentary by E. TUCCI.
[160] The current numbering of art. 234 TCE is 267 TFEU.
[161] *Productores de Música de España* v. *Telefónica de España SAU,* ECJ, 29.1.2008, C-275/06, paras. 29 ff.

34/2002[162] the communication of the information asked by Promusicae could be authorized only for criminal investigation and, in particular, for the aim of public security and national defence. This implies that it could not be obtained for a civil proceeding measure. Promusicae counterclaimed that art. 12 of Ley 34/2002 on the duty of retaining customers' information should have been interpreted in accordance with many different provisions of European Directives 2000/31, 2001/29 and 2004/48, as well as with art. 47 of the European Charter of Fundamental Rights, protecting the right to an effective remedy in law[163].

The *Juzgado* could not move from this impasse and asked the European Court of Justice the following question: "does Community law, specifically Articles 15(2) and 18 of Directive 2000/31, Article 8(1) and (2) of Directive 2001/29, Article 8 of Directive 2004/48 and Articles 17(2) and 47 of the Charter permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service?"[164].

The answer of the European Court was, as we will see, not completely satisfactory.

The question posed by the Spanish judge was whether European law, in particular Directives 2000/31, 2001/29 and 2004/48, also in the light of the Charter of Human Rights, had to be interpreted as imposing a duty, for Member States, to implement an obligation to communicate personal data in the context of civil lawsuits.

The first observation of the European Court of Justice was that Community law has to ensure effective protection to intellectual property, especially in the information society. However, the Spanish court was worried that the provision of

[162] It refers to LSSI ("*Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico*") of 11 July 2002, with which European Directive 2000/31/EC was implemented in Spain.
[163] Art. 47 of the Charter of Fundamental Rights of the EU's text is close to art. 24 of the Italian Constitution. In fact, the first part of art. 47 states: "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article".
[164] Cf. ECJ, C-275/06, cit., par. 34.

art. 12 of Ley 34/2002 could prevent this protection. This law was created to implement Directive 2000/31; but art. 12, instead, implements the protection of privacy, as required by Directives 95/46 and 2002/58 (the latter is expressly related to the processing of personal data in the electronic communications sector)[165].

The European judges clarified that the disclosure requested by Promusicae involved the making available of users' personal data, information to be considered as relating to identified or identifiable natural persons, as described by the definition of art. 2(a) of Directive 95/46[166]. The data stored by Telefónica was a processing of personal data as meant by art. 2 of Directive 2002/58, read together with art. 2(b) of Directive 95/46. The communication asked by Promusicae was therefore inside the scope of Directive 2002/58.

Once clarified the framework, the Court explained that it had to be ascertained whether Directive 2002/58 precluded Member States to implement, with the scope to protect copyright, an obligation to communicate personal data in civil proceedings. If this was not the case, it had to be considered whether this obligation followed from one of the other Directives mentioned by the Spanish judge (2000/31; 2001/29; 2004/48). If this was not the case either, the European Court should have considered whether, starting from the European Charter of Human Rights, other rules of the Community law would require a different reading of the mentioned Directives.

The Court therefore started to analyze each of the three Directives.

As for Directive 2002/58, the Court considered art. 5(1) which provides that Member States must assure the confidentiality of electronic communications and of the related traffic data. Among others, there is the prohibition of the storage of personal data by persons other than the user, without the consent of the users. The same Directive provides also some exceptions related to persons lawfully authorized (art. 15(1)) and to the technical storage needed for the communication itself. Furthermore, art. 6(1) of the Directive states that stored traffic information must be erased or at least anonymized when it is no longer needed for the purposes of the

[165] ECJ, C-275/06, cit., par. 41-44.

[166] Article 2. Definitions: "For the purposes of this Directive: (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

transmission of the communication. Art. 6 considered the processing of traffic data for the requirements of billing or marketing services. These provisions do not concern the diffusion of the data to persons other than those acting for the providers. In particular, art. 6(6) concerns "the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes". Therefore does not relate to situations like the dispute between Promusicae and Telefónica.

The Court then considered art. 15(1) of the same Directive. The provision considers the feasibility of the introduction of legislative measures to restrict the confidentiality of traffic data, when this restriction constitutes a necessary, proportionate and appropriate measure to safeguard State security, defence, public security or the prevention, investigation and prosecution of criminal offences or of the unauthorized uses of electronic communications systems. However, none of these exceptions, which are those listed in art. 13(1) of Directive 95/46, can be related to civil proceedings. Neither can be related to the case of Promusicae and Telefónica the exception of the unauthorized use of the electronic communication systems, since it would concern questions of actual integrity or security of the system.

Nevertheless, art. 15(1) of Directive 2002/58 closes with an express reference to art. 13(1) of Directive 95/46. This latter provision authorizes Member States to implement legislative measures which restrict the obligation of confidentiality of personal data when this restriction is necessary, among other reasons, for the protection of the rights and freedoms of others (art. 13(1), letter g). According to the opinion of the European Court, since the article does not specify what rights and freedoms are concerned, the provision had to be interpreted as not excluding the possibility of protection of the right to property or other situations where authors seek to obtain the protection in civil proceedings. This meant that Directive 2002/58 does not preclude the possibility for Member States of laying down an obligation to disclose personal data in civil lawsuits. At the same time, however, art. 15(1) does not compel Member States to lay down such an obligation for the situation the same article lists (national security, crimes, and so on)[167].

[167] Cf. ECJ, C-275/06, cit., paras. 45-56.

Given that Directive 2002/58 does not itself require Member State to implement such a kind of legislation, the European Court started to analyze the three directives mentioned by the *Juzgado*.

The European Court noted that the purpose of these three directives was to protect industrial property, more in particular copyright. At the same time, the three directives prescribe that such protection cannot affect the protection of personal data[168].

Art. 8(1) of Directive 2004/48 expressly requires Member States to ensure that, in the case of proceedings concerning an infringement of an intellectual property right and in response to a justified request of the claimant, the competent judge may order to provide information on the origin and distribution networks of the goods or services which infringe the right. However, this provision, which must be read along with paragraph 3(e) of the same article, does not require Member State to lay down an obligation to communicate the data. Nor do art. 15(2) and 18 of Directive 2002/31 or art. 8(1) and (2) of Directive 2001/29 require such an obligation.

As to the question of fundamental rights, the Spanish court referred to arts. 17 and 47 of the Charter. The first concerns the protection of the right to property, including intellectual property, stating, at its second paragraph, that "[i]ntellectual property shall be protected". The second, as already seen, is about the right to an effective remedy. By referring to these articles, the *Juzgado* probably meant to understand whether an interpretation of the European Directives implying that Member States are not obliged to implement an obligation to communicate personal information in civil proceedings would lead to an infringement of the fundamental rights contemplated by arts. 17 and 47 of the Charter.

The European Court claimed that both the rights to (intellectual) property and to effective judicial protection are general principles of Community law. But, as the European Court immediately pointed out, another fundamental right was at stake in the case posed by the Spanish judge: the right to the protection of personal data and, hence, of private life. The same Directive 2002/58, in its recital n. 2, proclaims the respect for fundamental rights and the observation of the principles of the Charter. In

[168] See art. 1(5)(b) of Directive 2000/31; art. 9 of Directive 2001/20; art. 8(3)(e) of Directive 2004/48.

particular, the directive ensures the respect of arts. 7 and 8: the first guarantees the respect for private life; the second expressly proclaims the right to protection of personal data[169].

Following these considerations, the Court of Justice found itself in the difficult position of having to "reconcile the requirements of the protection of different fundamental rights, namely the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other"[170].

The European Court identified two main mechanisms which would allow, it its opinion, the balancing of these different rights. The first mechanisms was inside the Directive 2002/58, as well as in the three directives mentioned by the *Juzgado*. The former directive provides for rules that determine when and to what extent the processing of personal data is lawful and which safeguards are to be provided. The latter ones reserve the cases in which the measures adopted to protect intellectual property under their provisions can affect the protection of personal data. The second mechanism was to be found in the Member State's national provisions implementing those directives and in their application by the national authorities.

Indeed, directives necessary contain general provisions, which have to be applied to a large number of different situations in many different countries. This is the reason why directives' rules leave each Member State the essential discretion in the transposition, so that the legislation can be adapted to the various national situations. Therefore, in transposing European directives, the Member States must assure to rely on an interpretation of the directive which permits a fair balance between the different fundamental rights protected by Community law. Furthermore, when courts and authorities apply those rules they must not only interpret their national law in a way consistent with the European Directives, but also rely on an interpretation of them which would be consistent also with the mentioned fundamental rights and other general principles of Community law. Among these principles, the Court pointed out, is the principle of proportionality[171].

[169] Cf. ECJ, C-275/06, cit., paras. 57-65.
[170] Cf. ECJ, C-275/06, cit., par. 66.
[171] Cf. ECJ, C-275/06, cit., paras. 67-68.

In addition to this, the Court recalled that art. 15(1) of Directive 2002/58 imposes all the measures to be adopted in compliance with art. 6(1) and (2) of the Treaty on European Union[172].

In the light of all these considerations, the Court of Justice concluded what follows:

a. Community law (meaning Directives 2000/31, 2001/29, 2004/48 and 2002/58) does not require Member States to lay down an obligation to communicate personal data to ensure effective protection of copyright in the context of civil proceedings, in situations such as the one that originated the Spanish lawsuit;

b. at the same time, however, Community law requires that, in transposing those directives, Member States rely on an interpretation of them that allows a fair balance between the fundamental rights protected by the European legal order;

c. when implementing the national laws transposing European Directives, authorities and courts of Member States should ensure that they rely on an interpretation consistent with the Directives and, at the same time, they should make sure that they do not rely on an interpretation which is in contrast with the fundamental rights or principles of Community law, among which stays also the principles of proportionality[173].

[172] The current numbering of art. 6 TUE remains art. 6 TUE. The text of the article is the following: "1. The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties. The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties. The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions. 2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties. 3. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law".

[173] In 2009 a copycat of the Spanish case reached the European Court of Justice from the bench of the Austrian *Oberster Gerichtshof (LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v. Tele2 Telecommunication GmbH*, ECJ, 19.2.2009, C-557/07). The conclusion of the Court in this order was exactly the same reached in the Promusicae case (actually, it was a copy-paste!). For a commentary see L. DI MICO, *Il rapporto tra diritto di autore e diritto alla riservatezza: recenti sviluppi nella giurisprudenza comunitaria*, in *Il diritto di autore*, n. 1/2010, 1.

4.3.3. The Peppermint case: second round

a) February 2008: the decision of the Privacy Authority

In February 2008, following the Peppermint cases, the Privacy Authority delivered a decision on the processing of data made by Logistep[174].

The decision did not concern exactly the problem arising from the mentioned cases[175]: rather, it was concentrated on the question whether the processing made by Logistep, and the subsequent processing made by the law firm representing Peppermint, had to be considered legitimate or had been made in violation of d.lgs. 196/03.

The Authority divided the activity of Logistep in two different steps: 1. the collection and automated elaboration, also with reference to databases, of a countless number of personal data, obtained through the use of a software called "file sharing monitoring" (fsm) used by Logistep; 2. the request made to the Italian judicial authority, in a civil proceeding, to obtain from some ISPs the communication of personal identities of the users concerned.

As already mentioned, following the first orders of the Tribunal of Rome, some ISPs disclosed the real identities of users to Peppermint. In turn, the law firm representing the recording company sent hundreds of letters to alleged file-sharers asking for a sort of settlement. According to the letters and to the claim of Peppermint, Logistep's software had acquired users' data while they were using peer-to-peer systems; in particular it seems that recipients of Peppermint's lawyers' letters had a folder on their computer to which other users could connect to obtain music files.

The Authority specified that the exchange of files in the Internet had to be considered as "communication", since the notion states: "'communication' means

[174] Privacy Authority, 28.2.2008, published in Bulletin n. 91/February 2008; available at: http://www.garanteprivacy.it/garante/doc.jsp?ID=1495246. Already in September 2007, the Authority had issued a deliberation relating the conservation of electronic communications data. Probably due to the cases here summarized, the *Garante* wrote that providers were not allowed to give data requested by party inside a civil proceeding, cf. Privacy Authority, 19.9.2997, published in Bulletin n. 86/September 2007, available at: http://www.garanteprivacy.it/garante/doc.jsp?ID=1442463, at par. 5. The Authority confirmed this decision also in the opinion delivered on 17.1.2008, published in Bulletin n. 0/January 2007, available at: http://www.garanteprivacy.it/garante/doc.jsp?ID=1482111.

[175] The Authority wrote that a decision on this point had been already taken by the European Court of Justice, referring to the Peppermint case. In the opinion of the Privacy Authority, the decision of the European Court had to be interpreted as an exclusion of the possibility to disclose the data requested by copyright holders in civil proceedings, cf. Privacy Authority, 28.2.2008.

any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service"[176]. The existence of a "finite number of parties" distinguishes a private communication from a communication to the public. Even if a peer-to-peer system allows the communication to a very high number of people, this does not mean that the number is indefinite or absolutely not determinable. The communication is in fact directed to delimitated subjects, who can be identified. Furthermore, to have a communication to the public there should be simultaneity and uniqueness of transmission, which are missing in the case of peer-to-peer.

The *Garante* then described the activity of the fsm software, which Logistep had used on the networks of GNUtella and eDonkey. The fsm software, created through the manipulation of free software used to connect to P2P networks, allowed: the usual operations made with "normal" clients, except from the sharing of files; the storage of the information which is usually characterized by volatility, since normally is not necessary after the transmission of files; to match the activity of a user on P2P network to changing IP addresses, or changing provider (thanks to the monitoring of GUIDs). The software gave the possibility to keep trace of the availability of certain content on the network. It also allowed to verify the real possibility of acquiring the content through the download; to verify the digital signature of the content; to control its diffusion, checking the existence of previous activities of sharing (on the presumption that usually those who share a file had acquired that file through file-sharing as well).

The Logistep's software also allowed the collection of IP addresses, name and Hash value of the file, size of the file, user name, GUID, hour and date of download. This means that the software could ascertain from whom and when a file was offered for download, and from whom, when and for how long that file was actually copied. The software also recognized the attempts of users to change their IP addresses. Finally, it organized all these information into a database.

Even if the software did not make intrusive activities or the installation of softwares or other component on the users' computer, the Authority concluded that the processing made by Logistep had to be considered illicit. In particular, the

[176] Cf. art. 2, letter d), Directive 2002/58 and art. 4, letter l) of the Italian Privacy Code.

principle of "lawfulness" was violated, since the collection had been made without the existence of a legal reason. The processing also violated the principle of "purpose", since the systematic registration of data was made for different purposes than the use of peer-to-peer softwares. Good faith and transparency were also violated, since users did not know of the collection of their data. Subscribers were unaware of the collection of their data also due to the fact that they are not necessarily the persons who engaged in file-sharing. Last but not least, even the principle of proportionality had been violated, since secrecy of communication should be limited only when facing a right with the same importance and therefore not for a civil proceeding.

This processing was massive and widespread; it lasted for a prolonged period, with regard to a high number of persons. In this way Logistep could keep trace of the operations made by an indefinite number of single users, with regard to specified copyrighted contents.

For the way in which this collection of data had been made, the Authority considered it as an activity which is prohibited to private entities by art. 5, European Directive 2002/58, and art. 122, d.lgs 196/03.

For admission of the same lawyer of Peppermint, the software fsm aimed at monitoring and searching data that P2P users made available to third parties. But the use of these data is allowed only for the scope for which the data are made available, and not for further scopes such as those pursued by Logistep, Peppemint and Techland.

The processing was also vitiated as for transparency and fairness, given that no previous information on the collection or use of data had been given to the users. As we have seen in the previous pages, the Tribunal of Rome has considered these data as personal information related to identifiable users, who should have been informed of this further and unpredicted processing. With regard to this point, the Authority cited an interesting document of the *Article 29 Data Protection Working Party*[177]. In that document the group stated that no personal data can be collected in

[177] The *Article 29 Data Protection Working Party* has been established by Article 29 of Directive 95/46/EC. It is the independent EU Advisory Body on Data Protection and Privacy. It is made up by representatives of national Privacy Authorities. Its tasks are more or less the same we have seen for the Italian Privacy Authority, but with regard and application to the entire EU territory. For further information, see http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

case the data subject has not been rightly and previously informed in a transparent way, on the possible methods of control and on the identity of the person processing the data. This information shall be given before the collection starts and before the data subject gives her personal data through the download[178].

The *Garante* added that the second phase of the processing of data (the sending of the letters) was done using personal data which had been illicitly collected. Therefore, following the above summarized reasons, under arts. 143 and 154 of the Privacy Code, the Authority enjoined Peppermint, Techland and Logistep from any further use of the alleged file-sharers' data. The Authority also ordered the three companies to erase the data within the end of March of the same year.

b) March 2008

Peppermint and Technland were probably not persuaded of the previous decisions and applied for another order from the Tribunal of Rome[179]; the decision was taken in March 2008. This time, the two companies sued Tiscali s.p.a., another ISP. As in the previous cases, the request of the claimants was to obtain Tiscali's customers' data, who had allegedly infringed the copyright hold by Peppermint and Techlands through the use of file-sharing programs.

Tiscali's counterclaim contained many objections. First of all, the claimants' request was not admissible because it lacked instrumentality and it could not anticipate a subsequent complete lawsuit to the provider[180]; moreover, the request could not be executed since it would violate users' privacy. The copyright holders had not given proof of an actual copyright infringement. In any case, the claimants would have nevertheless been concurrently liable in this infringement, since they had not sued the producers and suppliers of these file-sharing programs.

The Privacy Authority stepped in the process, as well as Codacons and Adiconsum[181], the most important Italian consumers' rights associations. The three

[178] The complete document (Working document on data protection issues related to intellectual property rights, January 18, 2005) can be found at http://www.garanteprivacy.it/garante/document?ID=1497279.
[179] Trib. Roma, ord., 17.3.2008, cit.
[180] There could not be a subsequent request: once the ISP disclosed the requested data, no other actions against the same ISP would be needed.
[181] Codacons is an acronym which stands for "*Coordinamento delle associazioni per la difesa dell'ambiente e dei diritti degli utenti e dei consumatori*", meaning "Coordination of organizations in defense of environment and of users' and consumers' rights". It was created in 1986 and it is, as it can

entities asked for the rejection of the request, due to a violation of consumers' privacy. Adiconsum also requested the judge to ask for a judgment on the constitutionality of art. 156*bis*, L. 633/41 in front of the Constitutional Court. In the opinion of Adiconsum, that article would be in contrast with art. 15 of the Constitution on the freedom and secrecy of correspondence and of any forms of communication. The association also wanted the judge to ask for a preliminary ruling by the European Court of Justice, on the existence of a duty for Member States to grant the disclosure of personal data on a civil proceeding on copyright infringement.

The judge clarified that, thanks to Logistep's action, users had been identified by a username/nickname and a GUID code; files had been identified through the Hash value and computed through the IP addresses. As usual, the claimants requested the judge to order the ISP the disclosure of its customers' data. The two claimants argued that the Italian implementation of Directives 2001/29 and 2004/48 was defective. In particular, the fact art. 156*bis* does not mention third parties, such as ISPs, among the possible receivers of a judicial order of disclosure was an omission in the enactment of Directive 2004/48. In the judge's opinion, however, the implementation of art. 8 of Directive 2004/48 had been a literal transposition, with no possibilities to have mistakes.

The judge considered the request of the claimants to be a discovery request. This means that, through the application of art. 156*bis* the claimant could obtain some evidence for a subsequent process, but not an injunction. This provision is based on two rationales: on the one hand the need to compensate the information asymmetry in the intellectual property enforcement process; on the other hand the increase of efficiency in the protection against counterfeiting.

The instrumentality of the claimants' request had to be considered with regard to a possible process in which the evidence found through the discovery could be used and not with regard to an eventual complete process against the ISPs, to be considered as an extension of the precautionary measure phase. For the same reason

be understood from its name, an "association of organizations" and it operates in many different sectors, including public services, justice, education, telephone services, health services, copyright (see www.codacons.it). Adiconsum is a consumers' association founded in 1987 by the labor union CISL. The organization negotiates the defense of consumers, against unfair commercial practices, frauds, and so on (see www.adiconsum.it). Both the organizations have also advisory power with regard to the Government and the Parliament, for the adoption of regulation regarding consumers.

it did not matter the existence of a *periculum in mora*; rather, it was important to consider the possibility that the evidence could disappear while the party are waiting for the lawsuit to commence. There might the possibility, given the way file sharing works and the high number of people using it, that the identification of every single consumer could be very difficult with time passing, according to the judge.

On the issue of the conflict between information privacy and copyright enforcement, for which the *Garante* and the consumers' associations had entered the lawsuit, the Tribunal of Rome noticed that there had been a decision by the European Court of Justice, which is the Promusicae case. After considering all the European norms, which could play a role in the controversy between Peppermint, Techland and Tiscali, the Tribunal of Rome recalled the Promusicae case and quoted the conclusions of the European Court of Justice[182]. The Tribunal acknowledged that the decision of the European Court had actually posed on the national judge the burden of balancing the conflicting interest, namely information privacy safeguard and intellectual property protection.

The Italian norms to be considered are:

- art. 4 of the Privacy code, giving the definition of "data processing";
- art. 24, letter f), of the same Code, which allows the processing of data without the data subject's consent to enforce a right in front of a judge;
- art. 123, of the Code, which prohibits the storage of traffic data;
- art. 132 that provides the duty to store traffic data for twenty-four months for the investigation and repression of crimes; and of other twenty-four months for the same reasons for some particular crimes.

Analyzing these norms, the Tribunal concluded that art. 132 of the *Codice della Privacy* was a special provision if compared to the one contained in art. 24, letter f). In particular, the fact that the Italian legislator considered the possibility of a longer period of storage only for crimes prosecution leads to the conclusion that exceptions to the need for data subject's protection should be applied only for that kind of processes.

The Italian legislator chose to limit the protection of personal data only to criminal cases. This choice is compatible with the interpretation given by the

[182] See Trib. Roma, ord., 17.3.2008, cit., 1740.

European Court of Justice in the Promusicae decision, where the Court said that there is no duty for the Member States to impose the disclosure of information in civil proceedings. Hence, in the Tribunal's opinion, the balancing between the two rights had already been done by the legislator. The two are indeed fundamental rights: the enforcement of intellectual property shall prevail on privacy only when there are public interests which are presided by the existence of criminal rules and penalties. On the contrary, when the only violated interest is the one of the copyright holder, personal data protection needs to be prevailing.

The national judge must interpret the national law in compliance with Community law and with the fundamental rights, as well as in compliance with the principle of proportionality indicated by the European Court. Therefore the Italian judge has to take note of the choices made by the legislator of not applying some measures of copyright protection when they violate the privacy right. This is exactly an expression of the proportionality of the means of enforcement and of the balancing made by the legislator.

Nonetheless, in the judge's view, the prevalence of privacy on the enforcement measures for intellectual property does not mean that the same rights are completely deprived of protection against file-sharing. The Tribunal suggested that peer-to-peer networks managers or file-sharing software producer could be sued to stop the infringement of copyright. The same judge cited the American system and the case of Napster as examples[183].

The judge finally concluded that granting the claimants' request would mean the disclosure of consumers' personal data without any consent, given also that they act on the Internet with the presumption of acting in anonymity. The disclosure would have violated their right to privacy and therefore the request of Peppermint and Techland lacked of admissibility. Therefore the claim was rejected.

[183] This suggestion of the Tribunal was criticized for being somehow in contrast with other provisions. In fact, as already seen, the Italian regulation for ISPs' liability provides that intermediaries cannot normally be held liable for the activity of users. Furthermore, producers and distributors of peer-to-peer software do not infringe any rule for the only fact of the production or distribution, since what is important is the way these software are used. Cf. A. SIROTTI GAUDENZI, *Violazione della proprietà intellettuale: non è ammesso il provvedimento di* discovery *in caso di* peer to peer, in *Giur. it*., n. 7/2008, 1744.

4.3.4 Fapav v. Telecom

In 2009, Fapav[184] sued the provider Telecom Italia s.p.a. to obtain a judicial measure that could order the ISP to take some particular measures in order to prevent the circulation of counterfeited copyright works[185].

Fapav had ascertained the existence of websites which made available copyrighted works illegally. Thirteen of these sites were Telecom's customers. Therefore in May 2009, Fapav had notified Telecom with the request to adopt the suitable measures, both technical and legal, to block the use of Internet connection for illicit behaviours. In particular, Fapav asked the ISP to block the access to those websites used for the illicit reproduction of copyrighted works and to communicate to the Public Authorities the information which would have allow the same Authorities to adopt suitable measures. Telecom replied in the negative.

Given that copyright infringement was persistent, Fapav sued Telecom to obtain a precautionary measure and, in particular, to obtain:

- that the ISP communicates to the Public Authorities the data needed to repress crimes as punished by arts. 171 ff., L. 633/41;
- that the ISP adopts the suitable measure to prevent or at least to impede the access to the mentioned websites;
- that the ISP informs its customers of the illegality of the reproduction of copyrighted works. It should also inform the customers that such conduct was contrary to the terms of services and that the prosecution of the conduct could lead to the termination of the contract;
- that the ISP is made subject to any other suitable measure to safeguard the claimant's rights.

Telecom's counterclaim contested the request of Fapav. In the lawsuit entered also S.I.A.E., sustaining Fapav's claim; AIIP[186], ASSOTELECOMUNICAZIONI[187] and the Privacy Authority entered to sustain Telecom's argumentations.

[184] Fapav (acronym for *Federazione Anti-Pirateria Audiovisiva*, meaning "Anti Audiovisual Counterfeiting Federation") was founded in 1988 as a non-profit association, with the aim to protect intellectual property, copyright, and related rights and to fight counterfeiting of audiovisual works. For more information see www.fapav.it.
[185] Trib. Roma, ord., 14.4.2010, in *Riv. dir. ind*., n. 3/2010, II, 248 with commentary by D. MULA.
[186] AIIP, Association of Italian Internet Providers, is an organization founded in 1995 and currently comprising forty-four different providers of telecommunicating services. See www.aiip.it.

In its counterclaim, Telecom had argued that the request should have been dismissed since in the lawsuit the websites' owners were missing, even if the request was to block the access to those websites.

Fapav contested the legitimacy of the intervention of the *Garante*. Under art. 154 of the Privacy Code the Authority has the power to check whether the processing of personal data is made in compliance with the applicable regulation. Furthermore, the Authority can also enter a lawsuit to question the unlawfulness of a processing of data used, for example, as evidence. Nevertheless, the *Garante*'s complaint of an illicit processing of the data used by Fapav was not grounded. Fapav had in fact used aggregated data (namely: number of accesses to every work in a given period of time), which could not allow the identification of IP addresses. IP had been anonimyzed through the erasure of part of the code. The claimant had therefore never known users' personal data; this was enough to conclude that there had been no processing of personal information as defined by art. 4, letter a), of the *Codice della privacy*. It was likewise admissible the request to order Telecom to supply the public authorities with the data needed for the repression of crimes.

Fapav's request to obtain an injunction was instrumental to a subsequent lawsuit in which the association would have asked Telecom for a damage compensation for the copyright infringement that the provider had favoured. Fapav said that d.lgs. 70/03, implementing Directive 2000/31, exonerates providers from liability since they do not enjoy a power of control on users, but they still have a precautionary duty (art. 16, d.lgs. 70/03). The judge held that the fact that a provider does not fulfil its duty makes the provider liable under art. 17, d.lgs. 70/03. The request of Fapav was therefore admissible, since it aimed at stimulating the intervention of Telecom.

As seen, the regulation of ISPs' liability can be found in arts. 14-17, d.lgs. 70/03. Under these provisions the provider has neither a duty to control the information which are transmitted or stored, nor a duty to actively search the existence of facts or circumstances from which an illicit activity could be inferred. Nevertheless, all the providers shall promptly inform the judicial authority or other

[187] Assotelecomunicazioni or Asstel it an association which represents the companies working in the information technology sector, supplying services of phones and mobile phones telecommunication. For more information see www.asstel.it.

surveillance authorities when they know the existence of suspected users' infringement (art. 17, co. 2, letter a). When requested, providers shall also promptly give to competent authorities the information they hold which allow the identification of users, in order to prevent illegal activities (art. 17, co. 2, letter b). They can be ordered by judicial authorities to take measures to prevent the infringement (arts. 14-16). They can be liable for the contents of their services when they did not obey to the request of the authority to impede the access to those contents or, when they were aware of the unlawfulness of the contents, they did not inform the competent authority (art. 17, co. 3)

The provisions applicable to Telecom as an ISP are only arts. 14 and 17, d.lgs. 70/03, since Telecom acts as a "mere conduit" provider. Therefore, the defendant did not have the duty to suspend the access to the website, of which illicit activity had been informed. This provision would be applicable only if Telecom was a hosting provider. Moreover, Telecom did not keep any of the conducts described in art. 14 which would have made the provider liable. Nor did Telecom receive any order from the competent authority to prevent users' infringement; hence it did not have the duty to suspend the access to the mentioned websites. Finally, Telecom did not receive from the authority any request for information needed to identify illicit activities.

For these reasons, the only violation which can be ascribed to Telecom is the lack in giving the information, with which it should have promptly supplied the judicial authority, after the notice received by Fapav. Telecom should have indeed inferred from the information given by Fapav that illicit behaviours were taking place and that, therefore, it had a duty to inform the competent authority. Furthermore, the provider should have not, as required by Fapav, interrupted the access to its services, since it is not a hosting provider and it is anyway contractually obliged to its supply.

Telecom is therefore responsible for the contents of its services, under art. 17, co. 3, d.lgs. 70/03. It is a joint responsibility with the websites' owners and users. Nonetheless, Telecom's responsibility comes from the violation of the duty to protect, and not from the violation of copyright. This means that it is not possible to subject the provider to measures aimed at repressing the violation of copyright

perpetrated by websites' owners and users. For the kind of violations which they aim to impede and repress, these measures are to be taken by the judicial authority. Hence, it is only the judicial authority that can ask a provider to supply further information or to block the access to the websites concerned. Only in these circumstances the provider has to give the information or to suspend the access to the website. It would be further liable in case it does not follow the order or request of the judicial authority.

Art. 163, L. 633/41 allows the exploitation rights' holder to obtain an injunction towards activities infringing her rights, even if these activities are providers' services. This provision does not entail another kind of responsibility for the provider, but it simply provides the possibility to obtain an injunction against the provider's services. Art. 163 does not oblige Telecom to interrupt or suspend its services more than d.lgs. 70/03 already does. The judicial authority cannot order this injunction if the process does not concern the investigation and repression of copyright infringement, made through the provider's services.

Therefore, the only order that the judge could made towards Telecom was to impose the provider to supply the judicial authority with the information obtained through Fapav's notice. In particular this information should be accompanied by the identifying data of websites' users and owners, which could be useful to complete the information contained in the notice.

For all the above summarized reasons the Tribunal partially granted the requests of Fapav and ordered Telecom to communicate to the public prosecutor of the Tribunal of Rome the information received by Fapav, concerning copyright infringement on cinematographic works, as well as the mentioned identifying data.

4.3.5 Critics, comments, and the request for balancing criteria

The Peppermint case, and its European brother Promusicae case, generated scholarly critics and comments. In particular, many authors have shown their doubts on the solution offered by the Italian court. Some of them had seen the preliminary ruling asked by the Spanish judge as a chance to obtain a clear criterion for the balancing of the conflicting rights. But they fell short of expectations while reading the conclusions reached by the European Court of Justice.

The way the Peppermint case was managed generated the fear that privacy, as well as freedom of speech, could undergo a chilling effect[188]. First of all, the activity of Logistep was criticized for being in contrast with art. 122 of the Privacy Code, which prohibits the use of an electronic communication network to access information stored in a users' computer, with the aim to store or monitor the users' activities[189]. This provision does not mention personal data, but it simply speaks of "information". Therefore no monitoring of the operation is allowed, let alone the monitoring of data which are considered to be personal. If we consider IP to be traffic data, the provision to be applied states that data should be erased after a given period of time. This strict regulation is undoubtedly linked to the delicacy of these data. In any case, when someone would like to monitor communication services for scopes which are not necessary for the supply of the service itself, this person shall notify this processing to the Privacy Authority (art. 37,co.1, letter d), d.lgs. 196/03). With these considerations in mind, scholars had already reached the conclusion of the *Garante*, later adopted by the Tribunal of Rome, which implies a prevalence of the protection of privacy over the enforcement of copyright[190]. Actually, some scholars claimed that the change in the opinion of the Tribunal was direct consequence of the intervention of the Privacy Authority[191].

In the first decisions, the Tribunal did not consider some important issues that later would have become fundamental for the resolution of the conflict between the two rights. The national and the European systems, in fact, allow neither the processing of data relating to electronic communication, nor their acquisition, communication or use. In the Italian system this can be traced back to arts. 2 and 15

[188] See for example R. CASO, *Il conflitto tra* copyright *e* privacy *nelle reti* Peer to Peer*: in margine al caso Peppermint – Profili di diritto comparato*, in *Dir. Internet*, n. 5/2007, 471, available at: http://eprints.biblio.unitn.it/archive/00001334/01/Roberto_Caso.Peppermint_Copyright_Privacy_1_0_dicembre_2007.pdf, 475.

[189] According to BLENGINO, SENOR, *Il caso "Peppermint": il prevedibile contrasto tra protezione del diritto d'autore e tutela della* privacy *nelle reti* peer to-peer, cit., 845-846, even if the decision of 16.7.2007 did not explicitly mention art. 122 of the Privacy Code, the Tribunal had nevertheless in mind the application of this provision.

[190] CASO, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto comparato*, cit., 476.

[191] BLENGINO, SENOR, *Il caso "Peppermint": il prevedibile contrasto tra protezione del diritto d'autore e tutela della* privacy *nelle reti* peer to-peer, cit., 836; SCORZA, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto interno*, cit., 466; FOGLIA, *La* privacy *vale più del diritto d'autore: note in materia di* filesharing *e di sistemi* peer-to-peer, cit., 599.

of the Constitution. The prohibition of processing can be overcome only by values or interests which have higher importance, such as for the common good[192].

IP addresses *are* personal information: they can lead to the identification of a person, as the same Peppermint demonstrated with the fact that they could notify more than 3.600 users with the "settlement letter". In order to reach the conclusion that IP numbers are personal data, it would have been sufficient to make reference to an opinion delivered in 2002 by the Article 29 Data Protection Working Party, according to which "IP addresses attributed to Internet users are personal data and are protected by EU Directives 95/46 and 97/66"[193]. Furthermore, in 2007 the Working Party also held that the collection of data, even if fragmented, still constitute processing of personal data when the person who collects them aims at identifying the data subject. Therefore it is not just the character of an information as "personal" to be taken into account, but also the purpose of the processing[194]. This approach aims at strengthening the protection of personal data. As for the cases here analyzed, it is unquestionable that Peppermint searched, collected, stored, and processed users' IP addresses and other data with the aim of identify them.

Anyway, the question whether IP addresses are personal data was not central to the analysed decisions. In fact, all the judges have somehow considered the need to have the users' consent. For example, the decision of 19th August 2006 held that the mere fact that a person enjoys file-sharing means an implicit consent to the knowledge of her IP number by the other file-sharers[195]. This would be an exception

---

[192] BLENGINO, SENOR, *Il caso "Peppermint": il prevedibile contrasto tra protezione del diritto d'autore e tutela della* privacy *nelle reti* peer to-peer, cit., 841.

[193] Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, adopted May 30, 2002, at 3. The document can be found at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-11. There seems to be still some uncertainty on the characterization of IP addresses as personal data by some scholars. See for example F. COUDERT, E. WERKERS, *In the Aftermath of the Promusicae Case: How to Strike the Balance?*, 18 International Journal of Law and Information Technology 50 (2008), 37 ff.

[194] The Working Party also gave the example of intellectual property rights holder who collect data for the enforcement of their rights. See Opinion 4/2007 on the concept of personal data, adopted June 20, 2007 at 15-17, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-6. The Working Party considered Recital 26 of Directive 95/46 stating "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person […]".

[195] A. MANTELERO, *L'idea del* peer to peer *fra tutela della privacy ed* enforcement *dei diritti d'autore*, in *Riv. trim. dir. e proc. civile*, n. 4/2008, 1488, fn. 38, notices that file-sharing users do not

to the necessary consent of data subject not contemplated by art. 24. The *Garante* has always asked for a strict interpretation of that article, stating that such exceptions are to be considered stringent, and cannot be extensively applied to other situations. The mentioned decision held that the processing of users' data was legitimate, since it aimed at enforcing or defending a right in front of a judicial authority, under art. 24, letter f). The decision of July 16, 2007, instead, considered that the application of this latter provision is feasible only in those cases where the claimant already possess the data and wants to use them to enforce her right, as long as this possess is legitimate[196]. In this case, the claimants did not have the data; rather, they sued the provider to obtain them. It was not a phase where their rights were enforced, but an anterior phase[197].

As already noted, the fact that IP addresses were personal data was, in the end, not questioned. Indeed the majority of the decisions analyzed the conflict between the right to data protection and the right to enforce copyright. It has been said that copyright is a noble right, since it is based on creation. Exploitation rights are not so noble, since linked to the economic side of creation. Both of them, anyway, have to bow in front of personal data protection, which, as seen, is also constitutionally granted[198].

As for the more delicate question of the balancing, an author has stressed the interesting point that the resolution of the conflict has been given by the Italian judges through the coordination of specific norms and not with reference to general principles. In the author's opinion this could mirror the conception of privacy, which

communicate their IP and GUID codes expressively, rather they are automatically detected by softwares such as the one of Logistep.

[196] MANTELERO, *L'idea del* peer to peer *fra tutela della privacy ed* enforcement *dei diritti d'autore*, cit., 1489 is of the same advise. For a critic of this interpretation see instead SCORZA, *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto interno*, cit., 469. Nevertheless, the interpretation of letter f) is fundamental, since with a too wide interpretation a person could for personal data of another subject, on the base of a possible future lawsuit. This would undermine the protection of personal data; see *Ibidem*, 469.

[197] BLENGINO, SENOR, *Il caso "Peppermint": il prevedibile contrasto tra protezione del diritto d'autore e tutela della* privacy *nelle reti* peer to-peer, cit., 844. The Authors claim that in this sense, the interpretation given in the decision of 17th March 2008 is more coherent, since the Tribunal considered art. 156*bis* as a discovery tool. It should not aim at identifying the alleged infringer, but at detecting the evidence needed in a subsequent lawsuit.

[198] BLENGINO, SENOR, *Il caso "Peppermint": il prevedibile contrasto tra protezione del diritto d'autore e tutela della* privacy *nelle reti* peer to-peer, cit., 849-850.

is not seen as a fundamental right yet, but, rather, as a limit to other rights[199]. Another scholar has pointed out that the existence of a right to privacy or to anonymity should not be seen as a picklock against rules punishing infringing behaviours; at the same time, however, intellectual property rights' protection tools cannot be considered as a way to prejudicially intrude into the protection of personal information[200].

In this framework, an author has considered art. 42 of the Italian Constitution. The second part of this article proclaims that private property, to which intellectual property is often traced back, is recognized and granted by law. Law also determines the limits to which property is subject in order to ensure its "social function". With this provision in mind, the mentioned author wrote that limits to intellectual property rights should be granted when those rights collide with other constitutional values which are opponents to market freedom. Among these latter rights he mentions also privacy[201].

As mentioned, the intervention of the European Court of Justice in the Promusicae case had been seen as a possibility to obtain a clear definition and solution for the conflict between personal data protection and copyright enforcement. The constitutional relevance of both the rights, confirmed by their mention in the European Charter of Fundamental Rights, obviously increases the difficulties in finding a right and stable solution to the conflict. Moreover, the delicacy of this contrast imposes a particular caution in determining a "one-fits-all" solution. In this sense, an author has noted that it would be more appropriate to apply an approach considering a concrete balancing of the interests at play, rather than a solution based only on the nature of the protection (civil vs. criminal law)[202]. This is particularly true given that the interests at play are of constitutional relevance and should therefore enjoy the same level of protection. For this reason it would be easier to

[199] DE CATA, *Il caso "Peppermint". Ulteriori riflessioni anche alla luce del caso "Promusicae"*, cit., 443.
[200] LATTANZI, *Protezione dei dati personali e diritti di proprietà intellettuale: alla ricerca di un difficile equilibrio*, cit., 248.
[201] G. SCACCIA, *Il bilanciamento degli interessi in materia di proprietà intellettuale*, in L.C. UBERTAZZI (ed.), *AIDA - Annali italiani del diritto d'autore, della cultura e dello spettacolo*, vol. XIV, Milano, 2005, 205-206.
[202] MANTELERO, *L'idea del* peer to peer *fra tutela della privacy ed* enforcement *dei diritti d'autore*, cit., 1495. According to a promintent Italian scholar, the same idea of protecting personal data should somehow consider a case by case approach. Different contexts can give different meanings to the same data. Cf. RODOTÀ, *Repertorio di fine secolo*, cit., 221.

apply a "procedural balancing rule", involving for example the principle of proportionality[203].

As the European Court itself recognized, the two conflicting interest should be reconciled. It has been claimed that a complete reconciliation is not always possible. Attention should be paid to the practical case, since in some instances one party's rights shall be limited in order to ensure the other party's right is not impaired. But "any restriction must not go beyond what is necessary for that purpose, and a fair balance must be struck between the conflicting rights. Thus reconciliation is closely linked to balancing/proportionality"[204].

This is true also in the light of the continue evolution of both the two rights and the technologies linked to them, which cannot possibly be completely defined right now. The decision finally taken by the Tribunal of Rome, as well as the content of the Privacy Authority's judgment, are probably strongly related to the fact that the violation of privacy was made through electronic communication networks. The capabilities of this kind of tools are obviously much bigger than those of analog instruments[205]. Therefore, privacy is different according to different scenarios.

The extent of the *Promusicae* decision of the European Court has been interpreted in three different ways: some authors claimed that the decision was in favour of intellectual property enforcement[206]; other authors said that the decision did not actually lean towards any solution, leaving to the Member States holding the baby[207]; finally, some others considered the sentence as a win for the protection of personal data[208].

---

[203] SCACCIA, *Il bilanciamento degli interessi in materia di proprietà intellettuale*, cit., 203-205.
[204] X. GROUSSOT, *Rock the KaZaA: Another Clash of Fundamental Rights*, 45 Common Market Law Review 1745 (2008), 1761.
[205] R. CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano*, in *Dir. Internet*, n. 5/2008, 470, available at http://eprints.biblio.unitn.it/archive/00001637/.
[206] MANTELERO, *L'idea del* peer to peer *fra tutela della privacy ed* enforcement *dei diritti d'autore*, cit., 1492 ff. Even if with reference to the copycat sentence on the Austrian case, it holds the same opinion also DI MICO, *Il rapporto tra diritto di autore e diritto alla riservatezza: recenti sviluppi nella giurisprudenza comunitaria*, cit., 2, where the author claims that the decision of the European Court seems to favour the needs to protect copyrithg on the respect of the right to personal data.
[207] "In essence, copyright law does not take supremacy over […] the right to privacy", cf. S. KIERKEGAARD, *ECJ rules on ISP disclosure of subscribers' personal data in civil copyright cases – Productores de Música de España (Promusicae) v Telefónica de España SAU (Case C-275/06)*, in 24 Computer Law & Security Report 268 (2008), 273; CASO, *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano*, cit., 468-469; COUDERT, WERKERS, *In the Aftermath of the Promusicae Case: How to Strike the Balance?*, cit., 51: "the 'hot potato' was passed on to the Member States". See also M. KOŠČÍK, *Privacy Issues In Online Service Users' Details*

The decision of the Court of Justice did not come up to the expectation of the scholars. As many of them have pointed out, the ruling is a sort of "non-decision", meaning that the Court did not specify which of the rights should prevail. The Court only said that there is no duty for the Member States to impose the discovery of users' data in copyright enforcement processes. In this vision, each Member State could apply its own preferences, in my view somehow undermining the attempts of uniforming the enforcement tools in the European context. Scholars have also suggested that the decision of the European Court should be considered as requiring additional exception to be added to those existing in Directive 2002/58. But this would also weaken the mentioned attempts to harmonize laws of Member States[209].

The only merit of the Promusicae decision is that the Court specifies in more than one occasion that each of the directives related to intellectual property yield the application of data protection directives.

The opinion of the Advocate General Kokott was probably more precise and concrete than the solution reached in the sentence of the Court[210]. The Advocate considered that Community law allows Member States to introduce a duty to disclose personal information for criminal matters. For civil proceeding Member States *may* provide for personal data to be communicated to State authorities, but are,

---

Disclosure In The Recent Case-Law. Analysis of Cases Youtube v. Viacom and Promusicae vs. Telefonica, 3 Masaryk U. J.L. & Tech. 259 (2009), 264 ff., who guesses that those awaiting a clear definition of the balancing should have been disappointed by the European Court ruling. Other scholars welcomed the decision more optimistically: "I do not share [Ip lawyers' critics]. This judgment is unsurprising and makes perfect sense to me", cf. GROUSSOT, *Rock the KaZaA: Another Clash of Fundamental Rights*, cit., 1758.

[208] A. TROTTA, *Il traffico telefonico fra la tutela del diritto d'autore e quella della* privacy, in *Dir. Industriale*, n. 1/2008, 76. "Th[e] judgement does not appear particularly helpful to the Spanish court […] it appears that Member States are permitted to decide for themselves what the correct balance should be […] The ECJ took a somewhat vague position", cf. K. BRIMSTED, G. CHESNEY, *The ECJ's judgement in Promusicae: The unintended consequences – music to the ears of copyright owners or a privacy headache for the future? A comment*, in 24 Computer Law & Security Report 275 (2008), 277. The same authors also criticizes the inclusion of "name and addresses" under the definition of "traffic data", see *Ibidem*, 278.

[209] BRIMSTED, CHESNEY, *The ECJ's judgement in Promusicae: The unintended consequences – music to the ears of copyright owners or a privacy headache for the future? A comment*, cit., 277. Cf. also COUDERT, WERKERS*, In the Aftermath of the Promusicae Case: How to Strike the Balance?*, cit., 61. "By allowing Member States to refuse the disclosure of personal traffic data related to copyright infringements for the purpose of bringing civil proceedings, the ECJ's judgment may lead to a further fragmentation of the law, in which some Member States allow such use but others do not". Quatation from C. KUNER, *Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice*, 5 European Intellectual Property Review 199 (2008), 202. Moreover see GROUSSOT, *Rock the KaZaA: Another Clash of Fundamental Rights*, cit., 1763 ff.

[210] Opinion of Advocate General Kokott, Case C-275/06, delivered on July 18, 2007, available http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006CC0275:EN:HTML.

nevertheless, not obliged to do so. In particular Kokott wrote that the possibility to disclose personal data can be restricted to very serious copyright infringement, as those aiming at profit or anyway deeply undermining the profit possibilities of copyright holders. In fact, in the opinion of the Advocate, copyright protection is a public interest that European Union has defended many times. Therefore, given the importance of copyright, even if the interest to be protected is a private one, its protection can anyway considered as fundamental. At the same time, however, file-sharing for private use, without profit making, cannot be considered as a real threat to copyright protection, taking also into account the controversial opinions on the effects of file-sharing on copyright profits[211].

To reach this conclusion, the Advocate considered a restrictive interpretation of art. 15, Directive 2002/58. The entire directive shall be considered a "*lex specialis*", since it regulates the specific sector of personal data in electronic communications[212]. However, the Court did not apply the same reasoning. Art. 13 of Directive 95/46 should be interpreted broadly: each Member State can include the protection of property rights in civil proceedings among the exceptions which allow the disclosure of personal data. In this way, the European Judges lowered the protection of personal information, since they did not stress the necessary presence of a pressing social need for the application of such measure[213]. As noted by the Advocate General, the question is when a threat to intellectual property rights imposes a necessary measure within a democratic society. It is at this point that the principle of proportionality reminded by the European Court comes into play[214]. The role of judges is thus fundamental. As scholars have pointed out "[i]ntervention by public authorities, acting as the guardians of fundamental rights […] appears crucial for any mechanism that is trying to implement a balance between the different interests at stake"[215].

Starting from the same points, the Advocate General and the Court of Justice reached two somewhat different conclusions. Even if both concluded that there is no

[211] Opinion of Advocate General, paras. 105-106; 119-121.
[212] Cf. Opinion of Advocate General, paras. 85-89.
[213] COUDERT, WERKERS, *In the Aftermath of the Promusicae Case: How to Strike the Balance?*, cit., 64.
[214] COUDERT, WERKERS, *In the Aftermath of the Promusicae Case: How to Strike the Balance?*, cit., 65-67.
[215] Quotation from COUDERT, WERKERS, *In the Aftermath of the Promusicae Case: How to Strike the Balance?*, cit., 71.

duty of disclosure of personal data in civil proceeding, the reasoning is different. The difference springs from the interpretation of art. 15(1) of Directive 2002/58, which makes reference to art. 13 of Directive 95/46. Art. 15(1) embodies a list of exceptions to the prohibition of storage and disclosure of personal traffic data on the Internet. According to its wording, the restriction to personal data protection must be "a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC". The reference to art. 13 was interpreted by the Court as the possibility to adopt legislative measures to restrict personal data protection when this is necessary, *inter alia*, for the protection of the rights and freedoms of other. As seen, the Court reasoned that, since "rights and freedoms" are not specified, they can include also the right to (intellectual) property. Therefore, the Community law does not compel but does not prohibit either Member States to lay down an obligation to disclose personal data in civil proceedings.

As said, the Advocate General interpreted art. 15(1) in a different way and, in particular, as not including the exception "for the rights of others". As previously mentioned, Directive 2002/58 is a *lex specialis* since it is related to electronic communications: for this reason the exceptions considered by art. 13(1) of Directive 95/46 are applicable only insofar as they are explicitly mentioned in art. 15(1). The explicit mention of art 13(1) by art. 15(1) does not clarify that non-listed exceptions are applicable (such as the protection of the rights and freedoms of others).

Some scholars have claimed that the possibility to disclose personal data could be linked also to civil proceeding under the provision of art. 24 of the Constitution, concerning the right to be heard in court for the protection of one's juridical situation. Given the constitutional protection of these rights, it would be of the same rank of the right to privacy, especially when the violation is a serious one[216].

Given all the constitutional interests which are at stake, once again the balancing should be made with an eye kept on adequacy and proportionality.

[216] M. GAMBINI, *Diritto d'autore e tutela dei dati personali: una difficile convivenza in Rete*, in *Giur. it.*, n. 2/2009, 512-513.

Therefore, the solution should be made case by case. It emerges also from the European Court's decision that privacy cannot always prevail. The same is nevertheless true also for intellectual property rights.

Chapter 5
Balancing conflicting rights: final remarks

"*It is precisely this constant search for a balance between the fundamental rights of each individual which constitutes the foundation of a 'democratic society'*".
[ECHR, *Chassagnou v. France*, April 29, 1999, par. 113]

5.1 The solutions adopted in the considered systems: giving an hypothesis

In the previous chapters I tried to give a sufficiently deep and complete account for what has being going on in USA, Canada and Italy, with regard to the field of interest. The current chapter would like to be a reasoned summary of the previous ones, at the same time providing some thoughts on the meanings and rationales behind the illustrated scenarios. The scope is to underline convergences and divergences in the solutions adopted by judges, taking into account the case studies developed in the previous pages. This would provide the foundations upon which I will build my hypothesis.

First of all, it is worth mentioning that USA and Italy have a specific provision under which a copyright holder can ask a judge to order an ISP to collaborate for the enforcement of copyright. On the contrary, the Canadian system relies on the subpoena provision applicable to every kind of civil proceeding[1]. We nevertheless know that USA copyright holders have been forced to use the usual "John Doe" tool, in this sense getting closer to the Canadian position. Furthermore, from another point of view, Canadian and USA approaches are closer between them than they are with respect to the Italian one[2]. In fact, in order to determine whether the disclosure of data should be granted to the claimant, Canada and USA apply a test constituted of multiple requirements that the claimant has to meet. On the contrary, the Italian approach requires only the existence of two elements, which are quite easy to demonstrate in the case of file sharing.

[1] USA: 17 U.S.C. § 512(h), known as the DMCA subpoena. Italy: art. 156*bis*, L. 633/41. Canada: Rules 233 and 238 of the Federal Court Rules.
[2] This is probably due to the fact that both the systems derive from the British one.

Before analyzing the way the decisions were taken, I shall try to sketch the differences in the solutions reached by courts in the different countries. It is clear that the solutions given vary not only among the considered systems, but also within each system. This is obviously a result of different interpretation of the rules relating to copyright and privacy and, more generally, is a typical outcome of the interpretative role proper of judges. Despite the mentioned divergences, we can outline a main line of decision for each of the three systems[3].

For what USA are concerned, the grater number of cases are solved in favor of copyright. This is true independently from the opposing right taken into account, i.e. anonymity and/or privacy. In the Canadian scenario, even if the sample is really limited, we can easily say that information privacy prevails on copyright. Finally, for what Italy is concerned, the majority of decisions was favorable to privacy.

In the chapter concerning the American system I have analyzed the path followed by the recording industry. As seen, despite the existence of the DMCA subpoena, claimants have been forced to switch to "John Doe" processes in order to have a chance of obtaining users' identities. This approach has sometimes led to the application of a test which includes the following factors: (1) whether plaintiffs have made a concrete showing of a *prima facie* claim of actionable harm; (2) the specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) a central need to obtain the subpoenaed information to advance the claim; and (5) the party's expectation of privacy[4].

The Canadian approach has considered the following criteria:

a) "the applicant must establish a *prima facie* case against the unknown alleged wrongdoer;
b) the person from whom discovery is sought must be in some way involved in the matter under dispute, he must be more than an innocent bystander;
c) the person from whom discovery is sought must be the only practical source of information available to the applicants;

[3] In the next paragraphs I shall try to give a plausible explanation for the way in which decisions were taken. I shall here only give a report of the different solutions..

[4] Cf. *Sony Music Entertainment*, cit., 564-565; *Arista Records, LLC v. Does 1-16* ,cit., 12. I am conscious that not all the considered cases have applied this test; nevertheless I find it useful to consider it, for the scope of this chapter.

d) the person from whom discovery is sought must be reasonably compensated for his expenses arising out of compliance with the discovery order in addition to his legal costs;
e) the public interests in favour of disclosure must outweigh the legitimate privacy concerns"[5].

The Italian application of precautionary measures requires only two elements: *fumus boni iuris* and *periculum in mora*, meaning a summary finding that 1) the claim is founded and 2) the danger that the right may be impaired by the lapse of time.

In my opinion all these approaches, even if different in some aspects, still have something in common. Firstly, it is particularly interesting that, even if none of the three provisions regarding disclosure of third party's documents or data mentions the need to consider third party's right to privacy, judges have nonetheless always taken this issue into consideration. This is probably due to the fact that users' privacy has always been used as a counterclaim by defendants.

The second point I would like to stress is that all the considered provisions leave a lot of space for judge's interpretation. This is probably the reason why privacy has been able to have a so important role in the balancing process. For example, as for the USA test, the expectation of privacy is a concept whose borders are not well defined[6]. The same can be said about letter e) of the Canadian test. How can a judge easily decide whether the disclosure of the data is more important of the privacy concerns? The Italian approach might be the least discretional among the three, considering that there is no clear reference to such a concept like "privacy". Nevertheless, art. 156*bis*, co. 3, L. 633/41, states that, in ordering the disclosure, the judge shall consider the necessary measure to protect confidential information[7].

What is most appealing in these lawsuits is the conflict between copyright enforcement and users' information privacy (as well as anonymity). The previous chapters have demonstrated that such conflict exists, that it is persistent and absolutely challenging, regardless of the outcome of each single lawsuit. In my

[5] *BMG I*, paras. 13-14.
[6] This is demonstrated also by the attention that scholars have placed in this particular issue.
[7] The expression "confidential information" seems to me to refer more to questions of industrial secrets and business competition than to questions of privacy.

opinion, the strain under which judges find themselves in such situations is the expression of the tension existing not only between privacy and copyright; it concerns a bigger tension between copyright holders' rights and users' rights. The above mentioned discretion enjoyed by judges constitutes the arena where these rights have enough space for fighting. Judges are the arbiters of these fights, where there are no precise rules following which judges can easily determine who (better: which) is the winner.

In my opinion, given that there are no clear legislative solutions; judges have to apply their own ideas, perceptions, and conception of the institutions at play. It is clear that to some extent courts always intervene in such a way in their decisions. Judges are very far from being the *bouche de la lois* theorized by Montesquieu in the 18th century[8]. Indeed, when facing situations like the ones considered in this work, they are probably the furthest from this vision.

The main question I shall try to answer in the next paragraphs is: in solving the analyzed conflicts do judges follow the main policy or do they follow societal perceptions? My view is that in the selected cases judges found themselves divided between the two forces: on the one hand there is the perception of society; on the other the national policy. Is the perception of society able to intrude into the decision of the judges, who, consciously or not, follow this perception? In whichever way we answer these questions, judges are to be considered as either (both) policy makers or (and) law makers.

I am aware of the existence of deep and wide differences among the three considered legal systems. These differences concern many aspects of the creation and interpretation of law, as well as of the judicial selection and organization. Applying the classical subdivision between common law and civil law countries[9], USA and Canada have probably a more similar approach if compared with the Italian

[8] According to his view, "judges are no more than the mouth that pronounces the words of the law, mere passive beings, incapable of moderating either its force or rigor" (in the original: "*les juges de la nation ne sont, comme nous avons dit, que la bouche qui prononce les paroles de la loi, des êtres inanimés qui n'en peuvent modérer ni la force ni la rigueur*"); cf. C.L. MONTESQUIEU, *Œuvres complètes de Montesquieu: avec des notes de Dupin*, *Crevier, Voltaire, Mably, Servan, La Harpe*, Livre XI, Chapitre VI, Paris, 1838, 268.

[9] I am referring to the classification proposed by R. DAVID, C. JAUFFRET-SPINOSI, *I grandi sistemi giuridici contemporanei*, Padova, 1994, 17 ff. K. ZWEIGERT, H. KÖTZ, *An introduction to comparative law*, Oxford, 1998, 63 ff., give an overview of the different classifications proposed by the most prominent scholars in the field of comparative law.

one. The role of judges in each of these countries varies to great extent. Nonetheless the same notable author that proposed the just mentioned subdivision into families also wrote that the creative function of law is always hidden behind the surface of the interpretation of law[10]. Judges have necessarily to take a decision, even in cases where they do not have a rule, such as those considered in this work.

In every country judges have the role of creating law, to a greater or smaller extent depending on the system; but they always have this function[11]. Without pretension of giving a complete picture of the different judicial systems, it is enough to recall some peculiarities of the considered countries. For example, it is well known that in countries like Italy even if the judges create *de facto* law, these rules do not have the same power as those coming from the legislator. Things are different in the other two countries, where there is the rule of *stare decisis* that typically characterizes the common law jurisdictions[12].

Another important difference lays in the way in which judges are recruited. Italian judges are for the biggest part recruited through open competitive exams, as required by the Constitution (art. 106). Therefore, people usually choose to follow this career since the beginning ant till the end of their professional path[13]. In the American system, judges are appointed by the political system or elected by citizens, in this sense creating the need for a sort of feed-back towards the people who have chosen them.

What I would like to point out with these two examples is my awareness of the fact that the explanation I will try to give can be one of the many which might be advanced. The solution I will suggest is probably one of the concurring reasons which lead judges to follow one or another direction. After having showed the

[10] DAVID, JAUFFRET-SPINOSI, *I grandi sistemi giuridici contemporanei*, cit., 111.
[11] For an account of the role of judges in civil law countries, see DAVID, JAUFFRET-SPINOSI, *I grandi sistemi giuridici contemporanei*, cit., 110 ff.
[12] For a brief account of the rule of *stare decisis* in the USA, see DAVID, JAUFFRET-SPINOSI, *I grandi sistemi giuridici contemporanei*, cit.,377 ff.; A. GAMBARO, R. SACCO, *Sistemi giuridici comparati*, Torino, 2008, 160 ff. For the Canadian system: F.L. MORTON (ed.), *Law, politics and the judicial process in Canada*, Calgary, 2002, 395 ff. It should be noted, however, that there are psychological mechanisms under which previuous cases exercise a binding effect also in civil law countries, cf. for example G. SARTOR, *Legal Reasoning: A Cognitive Approach to the Law*, in E. PATTARO (ed.), *A Treatise of Legal Philosophy and General Jurisprudence*, Vol. 5, Dordrecht, 2008, 735 ff.
[13] For an explanation of the judicial system in Italy see G. DI FEDERICO (ed.), *Ordinamento giudiziario. Uffici giudiziari, CSM e governo della magistratura*, Padova, 2008; see spec. 173 ff. on the recruitment system.

conflict in the previous chapter, I am interested in understanding why these specific solutions have been given, the reasons behind them. This is particularly important for jurists who operate today, in what have been called "digital era". The selected cases are paradigmatic examples of the tensions created by digital technologies (better: by a specific use of those technologies), and of how the law reacts when facing technological evolution. I have chosen to illustrate those cases, and the conflicts they introduce, as a case study.

As previously mentioned, judges must decide the cases brought to them by the parties, even when an applicable norm is lacking. In the present times technologies seem to run increasingly faster than law. This means that judges face (and will probably continue to face) situations in which they have to decide on the basis of laws which are obsolete, which do not help in finding solutions because they were conceived for other, old times. When judges are in these situations, they exercise their discretion more than in other contexts. It is to these situations that my analysis should be applicable.

In trying to understand why judges lean towards a solution or another, I will take into account the concepts of social perception and of legal culture. I would like to comprehend if and how judges can be influenced in their decisions by the social/cultural perception of a concept like privacy. In the next part I will explain what I mean for social perception and for legal culture, and why I choose to consider these particular aspects.

The idea of legal culture can be used as a way to explain the differences among the so called "law in books" and "law in action"[14]. The concept of legal culture is not an easy one, and while explaining some mechanisms, it also brings some complications with itself[15]. Indeed, my aim would be to clarify whether judges

[14] This antithesis can be traced back to the fundamental works of R. Pound. Pound, which was the founder of what was later called "legal realism", and wrote extensively on the issue. Just to have an idea of his interest for interdisciplinarity and, in particular, for his attention to social framework, see R. POUND, *The need of a sociological jurisprudence*, 31 Annual Report American Bar Association 911 (1907). He wrote: "books are still full of the old method, even in those matters in which progress is making", *Ibidem*, 916. "The modern teacher of law should be a student of sociology, economics and politics as well. He should know not only what the courts decide, but quite as much the circumstances and conditions, social and economic, to which these principles are to be applied; he should know the state of popular thought and feeling which makes the environment in which the principles must operate in practice", *Ibidem*, 919.

[15] Cf. D. NELKEN, *Using the concept of legal culture*, 29 Australian journal of legal philosophy 1 (2004), 2.

are somehow influenced by the culture of privacy existing in the country in which they operate. In fact, judges do not leave as hermits; they are part, to a greater or lesser extent, of a given society. At the same time, in a globalized world such as the present one, considering cultures within national boundaries can have little sense[16]. Let us think of the particular world of the Internet. In the Internet there are no boundaries; reactions to an event can start from a country and have a great stir also on the other side of the globe[17]. Therefore, it might be more useful to consider the existence, for example, of an "Internet culture", including those using the Web, or of a more circumscribed "file-sharing culture", meaning the culture of those using file-sharing softwares. To this extent, a person can belong to different cultures at the same time[18].

Talking of national cultures in such an open environment can be useless or even misleading. Moreover, it should be noted that what is considers as "culture" or "culturally oriented" is often the product of stereotypes, of a distorted imagination. Even if we can talk of a particular culture, the same culture was probably different in the past, and will be probably different in the future[19].

The way I will apply the concept of culture does not tend to understand the way law should be interpreted. Rather, it seeks to understand "the range of considerations that actors routinely rely upon, sometimes implicitly, sometimes expressly, in their interpretation and application of the law"[20]. In particular, I ask

[16] NELKEN, *Using the concept of legal culture*, cit., 3. The same author nonetheless writes: "[w]hat does seem undeniable is the extent to which legal culture is becoming ever more what we could call 'relational'. With increasing
contact between societies there are ever more opportunities to define one's own legal culture in terms of relationships of attraction to or repulsion from what goes on in other societies"; *Ibidem*, 7.

[17] Just to give a couple of recent examples, let us think about the roar caused by the American bills of SOPA and PIPA (see J. VIJAYAN**,** *Protests against SOPA, PIPA go viral. Google, Wikipedia, Reddit, BoingBoing plan unprecedented Internet 'strike' Wednesday*, Computerworld.com, January 17, 2012, available at: http://www.computerworld.com/s/article/9223496/Protests_against_SOPA_PIPA_go_viral), or by the FBI action against the website Megaupload (see T. BRADSHOW, *Anonymous in revenge attack for MegaUpload shutdown*, Financial Times online, January 20, 2012, available at: http://blogs.ft.com/fttechhub/2012/01/anonymous-megaupload-ddos/#axzz1l2M8ZhJy; N. GOHRING, *Anonymous Retaliates for Megaupload Shutdown, Attacks DOJ, Others*, Pcworld.com, January 20, 2012, at: http://www.pcworld.com/businesscenter/article/248445/anonymous_retaliates_for_megaupload_shutdown_attacks_doj_others.html; L.TAYLOR, C. CONNELLY, *FBI shuts down Megaupload.com, Anonymous shut down FBI*, news.com.au, January 20, 2012, available at: http://www.news.com.au/technology/fbi-shuts-down-megauploadcom-charges-seven-with-online-piracy/story-e6frfro0-1226249114650).

[18] J. WEBBER, *Culture, legal culture and legal reasoning: a comment on Nelken*, 29 Australian Journal of Legal Philosophy 27 (2004), 31.

[19] NELKEN, *Using the concept of legal culture*, cit., 6.

[20] WEBBER, *Culture, legal culture and legal reasoning: a comment on Nelken*, cit., 34.

myself: what role can culture play in the decisions taken here as cases of study? I share the vision that law is continually refashioned to be applied to new circumstances, also due to changing social attitudes and practices. And the concept of culture could help in understanding how this refashioned interpretation occurs, while at the same time not specifying which interpretation of law is the correct one[21].

The existence of spaces of option and open clauses gives judges the room to exercise their discretion[22]. As said, the legislator is too slow to keep up the pace of technologies, forcing judges to apply old rules to new schemes. And even when this problem does not really exist, judges are sometimes in the middle of fights which solutions can be influenced by societal perception.

In the next paragraphs I will first give an account of the perception of privacy, as emerging by anthropological and sociological studies. I will then consider the policies applied in the different countries as for copyright and file sharing. Finally, I will seek to explain the reasons why solutions have been different in the considered systems, looking at scholarly works on judicial reasoning.

5.2 The perception and conception of information privacy in the three systems

As previously explained, my aim is to demonstrate that judges take their decisions accordingly (also) to the perception existing in the society in which they live. I will now make another statement. Judges are also influenced by the existing policies on a particular subject[23]. I mean that they rely their decisions not only on existing laws, but also on a wider framework of policies in which those laws are inscribed.

[21] WEBBER, *Culture, legal culture and legal reasoning: a comment on Nelken*, cit., 35. To me this means applying a merely descriptive approach.

[22] "[I]t may be said that there is no sensible standard for balancing conflicting fundamental rights. The judge has, in fact, a considerable degree of discretion in the balancing process which, therefore, leads to unconstrained subjectivity
or intuitionism. Besides, there is a value judgement of the court which is no longer related to the alternatives of a right or wrong decision. Weighing of values is said to be able to yield a judgment as to a result, but is not able to justify that result": GROUSSOT, *Rock the KaZaA: Another Clash of Fundamental Rights*, cit., 1761.

[23] By the term "policy" I refer to the architecture of regulations, meaning the general approach to a given subject matter followed by the players of the entire legal systems (i.e. governments, authorities, and so on). Therefore I shall not consider singular aspects of law, but I shall rather take into account a larger picture, the structure of the regulation.

There is a sort of circulation of thoughts and perceptions which, to put it simple, starts from society, passes through lawmakers and policymakers, and reaches judges. This dynamic is actually more complicated than what it may appear. The connections among these factors are many, in terms both of quality and quantity, and they all affect each other. Laws can modify the perception of a particular issue. Furthermore, the perception that people have of a given institute can be the source from which new statutes spring, which means that society (and its perceptions) can influence lawmakers. There is a sort of virtuous circle among these factors and judges are someway in the middle[24]. They can be thought both as lawmakers, especially in those countries where common law applies, and as policymakers, especially, I would say, when laws are not clear enough or are, let us say, "open".

Given these premises I shall now analyse the perception of information privacy in the three systems. Moreover, with reference to the "connection" just illustrated, I shall give an account of the policies related to privacy. Again, because of the way in which the connection shows itself, the two narrations will sometimes necessarily overlap. I like to call these two aspects the "perception" and "conception" of a given institution: perception meant as the cultural feeling and social attitude towards the institution; conception meant as the organic whole of laws and policies relating a specific institution.

Before starting to discuss divergences and convergences of the policies of the considered countries, it is worth noting the importance of technology in the adoption of every piece of legislation about data protection. In particular, starting in the Seventies, developed countries considered the necessity of legislating the new issue of computer technology. Thanks to formal and informal relationships among countries, as well as some supranational interventions, the core principles of data protection legislation were adopted by every system[25]. This is a point in common among the three systems; but correspondence among them does not go too far.

Moving now to the analysis of regulation, it can be inferred from the pages dedicated to the United States that in that country the legislation for the protection of

[24] Actually, the circle can also be "vicious". Let us for example think at those legislations enacted as a response to mass panic.

[25] BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, cit., 118-123, attributes the convergences in personal protection regulations mainly to the threat that technology put on society at that time.

privacy is a pattern of statutes. First of all, the regulation is divided among state and federal rules. This characteristic is undoubtedly source of disparity among the different states, which in turn means a lower protection of the right itself. In fact, despite an increasing number of statutes has been enacted in the last forty years also at the federal level, the American scenario lacks uniformity and coherence in protecting privacy. Furthermore, the intervention for the protection of this right has often been a consequence of specific events. This gives way to a fragmented legislation, which cannot handle all the situations since it is concentrated on a small piece of the whole scenario. This way of legislating, which can be conceived as a response to public concerns, seems to reinforce my statement that the way privacy is regulated is (also) a response of a cultural perception of the necessity to protect personal information.

Another characteristic of privacy law in the United States is the fact that, very often, rights which would be considered as autonomous in other countries are traced back to privacy. In this sense, the right to privacy is wide and covers an indefinite numbers of situations. Let us think, as examples, to the famous cases related to abortion or to the use of contraceptives. This wide perspective can at the same time strengthen and weaken the concept of privacy and its protection. Privacy can be strengthened by the fact that it is often invoked and applied as a defence: the more interests of the person are protected, the more the "core concepts" of privacy can be respected[26]. Nevertheless, the right to privacy can also be weakened by this wide approach, since if privacy is seen everywhere, then it is seen nowhere. It could become a sort of "jocker-right" to be used every time there is a situation to be defended and no precise right is violated.

With regard to the protection of privacy, Canadian and Italian systems are on closer positions when compared to the American scenario[27]. Both the Canadian and the Italian approach include (at least) one important all-encompassing statute, namely PIPEDA and the *Codice della Privacy*; Canada has also a *Privacy Act* dated 1985. Strict rules apply both to private and public entities, and consent is the basis for

[26] For "core concepts" I mean the right to be let alone, as well as the control over one's own information.

[27] For the policies of personal data protection of USA, Canada and some European countries, see the study of D.H. FLAHERTY, *Protecting Privacy in Surveillance Society. The Federal Republic of Germany, Sweden, France, Canada & the United States*, Chapel Hill, 1989.

processing personal data. Despite the criticism on consent, its forms of manifestations and its actual validity and efficiency, it can be affirmed that the existence of this principle is a definite index of the centrality that data subject and her will have. This is the main difference in the issue "opt-in vs. opt-out", even if, it is worth recalling it again, the effectiveness of data subject's consent in the protection of personal data is highly questioned[28].

Another indication of the differences between the approaches is the existence or non-existence of a dedicated Privacy Authority. As seen in the previous chapters, both in the Canadian and the Italian systems a specific Privacy Authority exists and its role has also been very important for the definition of the right to privacy in the cases described in the preceding chapter, as well as in other occasions where digital technologies constituted a threat to that right. In the USA the creation of an institution which controls the application of privacy regulation is quite new[29]. The "Division of Privacy and Identity Protection" is in fact the newest division of the Federal Trade Commission – Consumer Protection Bureau[30]. The Division, created only in 2006, "addresses consumer privacy and data security matters through aggressive enforcement, rulemaking, policy development, and creative outreach to consumers and businesses"[31].

[28] For an account of this critics, I shall make reference to the works cited in the previous chapters.

[29] See the article by M. ROTENBERG, *In Support of a Data Protection Board in the United States*, 8 Government Information Quaterly 79 (1991), 86: "It is clear that the time has come for Congress to address […] the protection of information privacy. […] the question is simply where to begin. The answer is to establish a Data Protection Board. The Board is the missing piece in the privacy protection framework of the United States". The need for an institution presiding privacy protection was felt also by some scholars. A part from the already cited contribution, as examples, see also FLAHERTY, *The need for an American privacy protection commission*, cit., and, more recently, R. GELLMAN, *An American privacy protection commission: an idea whose time has come…again*, 11 Government Information Quarterly 245 (1994).

[30] "The Division of Privacy and Identity Protection, the newest of the Bureau's divisions, oversees issues related to consumer privacy, credit reporting, identity theft, and information security. The Division enforces the statutes and rules within its jurisdiction, engages in outreach and policy development, and educates consumers and businesses about emerging privacy, credit reporting, and information security issues, as well as identity theft prevention and assistance. In addition, the Division analyzes the impact of current and potential legislative initiatives in the areas within its purview". cf. http://www.ftc.gov/bcp/bcppip.shtm. BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, cit., 170 ff, explaines why USA did not apply an institutional mechanism solely responsible for privacy. It seems that this solution was the result of the mediation among a high number of different authorities.

[31] Citation from *The President's Identity Theft Task Force Combating Identity Theft*, *Volume II: Supplemental Information*, April 2007, available at: http://www.idtheft.gov/reports/VolumeII.pdf.

The scarce relevance of this Division is testified by the fact that none of the decisions analyzed here ever mentions it. Clearly, the absence of references could be just a consequence of the fact that the Division is a new institution, and therefore had not yet given a real contribution to the issue at the time the analyzed cases were decided. But what is more interesting is that the Division not only was created just in 2006, but it is simply a division of another institution. In this sense, Canada and Italy seem to give more importance to the role of the privacy authority, creating a dedicated specific organism. This in turn means giving more importance to the right to privacy itself than the United States approach does.

Many studies have illustrated that privacy is a value of every society, even if the way in which this value is perceived and demonstrated vary greatly across countries. For example, anthropologists showed that also tribal populations have a sense of privacy and apply certain rules for its protection[32]. As mentioned, the perception of the right and the way in which it is protected can deeply vary among different nations. This is probably the proof that, despite the private sphere of people's life is everywhere considered as a value to be protected, the extent to which this protection is granted depends on the consideration given to privacy itself[33].

The protection established for privacy can be therefore thought as a reflection of the cultural perception and consideration of that value. It was claimed that "[p]rivacy law is not the product of logic […] It is the product of local social anxieties and local ideals"[34]. The same prominent scholar has suggested that a main difference between the European and the American approach comes from history. The Old World's view of privacy is related to honor as well as human dignity, giving importance to personality rights. The idea of America is instead more concentrated on the value of liberty, and on the intrusion made by the State in people's private lives. This is probably the reason why the most important and more comprehensive

[32] As an example see the contribution of ALTMAN, *Privacy Regulation: Culturally Universal or Culturally Specific?*, cit.

[33] With reference to US and Europe privacy legislations WHITMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, cit., 1160, writes: "[w]hat we must acknowledge […] is that there are, on the two sides of the Atlantic, two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly different laws of privacy". For an explanation of how USA Privacy Act of 1974 was the result of public concerns on privacy, see BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, cit., 65 ff. The same analysis is made with reference to Sweden, West Germany, and Great Britain,

[34] WHITMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, cit., 1219.

acts introduced in the United States aim at regulating governmental intrusion and control of privacy. The "reasonable expectation of privacy" is especially applied inside one's own home walls. Leaving those walls, protection lessens and lessens[35].

For what European regulation of privacy is concerned, it is worth recalling that at the beginning it was mainly a response to the integration process of Member States. The harmonization of personal information processing and circulation was a requisite to increase the smoothness in commercialization of goods and services within the European Union[36]. This is not the case for the regulation of privacy in Canada or the United States. In the latter, privacy law was more an effort to prevent from intrusion by new technologies, especially by the State. To this extent, it was claimed that the current framework of privacy protection in the USA is a "creation of lobbyists in Washington", and not an historical effect[37]. In the meantime, a prominent scholar has also held that in the US context "[c]ourts and policymakers frequently struggle in recognizing privacy interests, and when this occurs, cases are dismissed or laws are not passed. The result is that privacy is not balanced against countervailing interests"[38].

Canadian approach has been called a "middle ground" between Europe and USA, since based on "individual's sense of control". According to this view, Canadians are not concerned in disclosing their data; rather, they are concerned with the way in which their data are handled. It is the processing of data which raises privacy problems, because they do not want to lose their autonomy. Canada places

[35] See WHITMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, cit., *passim*, in which the author, analyzing France, Germany, and USA, gives a number of different historical explanations which gave birth to the current frameworks of privacy in the two continents. The author claims that the seminal article by Warren and Brandeis brought "continental privacy" into America, applying also the idea of "personality". Cf. *Ibidem*, 1204-1208.

[36] See, as an example, Recital n. 7, Directive 46/95/EC: "Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions".

[37] ROTENBERG, *Fair Information Practises and The Architecture of Privacy (What Larry Doesn't Get)*, cit., ¶ 27 (The author is skeptical about the vision that the protection of privacy in the United States is less accurate of the Eurpean one. He underlines how the introduction of European privacy law was mainly a response to market needs). For an account of the role of groups and lobbies in the making of privacy policies, see BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, cit., 145 ff.

[38] SOLOVE, *A Taxonomy of Privacy*, cit., 480.

strong importance on dignity, such as Europe, but in the meantime has a lot in common with USA[39].

In order to give a less naïve picture of the situation, I shall also introduce some counter-arguments against my idea. Indeed, looking at surveys and opinion polls, some authors have pointed to the fact that the US population is sensitive to the need to protect privacy[40]. This would imply that governmental policies do not reflect the cultural perceptions and needs[41]. At the same time, however, it is well known that lobbies can have a great impact on the legislation of a country. It is also well known that the processing and storage of personal information is of absolute importance for nowadays companies. And it goes without saying that a society like the American one has always been highly based on business and has always trusted the market. Therefore it is possible that, even if American people feel the necessity of protecting information privacy, lobbies do make such an effort or have such a power that social needs are overcome. In fact, despite the existence of a high number of bills and statutes concerning privacy, prominent scholars have demonstrated that in the United States there is a dominance of interests over the value of privacy[42]. But "[p]rivacy protection need not be measured against economic benefit and corporate riches. The equation mistakenly places individual liberty on the auction block"[43].

US citizens have a great consideration of values like freedom of speech and freedom of information. The existence of restrictions on these rights due to the need for protection of privacy might have been seen as a threat to the mentioned rights, which should be restricted only for determined and exceptional reasons[44].

Another implication that has to be considered for offering a more precise and consistent picture is the already mentioned connection among the two variables "policy" and "culture/society". Policy can be the expression of cultural perceptions. At the same time, cultural perceptions can also have their sources in governmental

[39] A. LEVIN, M.J. NICHOLSON, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 University of Ottawa Law & Tech. J. 357 (2005), 391-393.
[40] ROTENBERG, *In Support of a Data Protection Board in the United States*, cit., 80 and 84.
[41] On this point, with particular referenct to online privacy, see M.J. METZGER, S. DOCTER, *Public Opinion and Policy Initiatives for Online Privacy Protection*, 47 J. Broad. & Elec. Media 350 (2003).
[42] REGAN, *Legislating Privacy*, cit., xiii.
[43] ROTENBERG, *In Support of a Data Protection Board in the United States*, cit., 85.
[44] See the opinion of BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, cit., 137. Cf. also WHITMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, cit., 1209. In my opinion it should be stressed that privacy is often the pre-condition of free speech: for this reason the former should not be always be overcomed by the latter.

policies. To give an example, an Italian author claimed that the declamatory approach used in L. 675/2003 on personal data protection was a sort of expedient. In his view, this method was essential to allow a quicker metabolism of principles which had remained at the margin of legal culture and also of the social sensitivity of the country[45]. It has been claimed that "[w]e have intuitions that are shaped by the prevailing legal and social values of the societies in which we live. In particular, we have […] *juridified* intuitions –intuitions that reflect our knowledge of, and commitment to, the basic legal values of our culture"[46].

That privacy regulation reflects (also) cultural values has been proved by empirical studies[47]. For example, a study conducted in the early 2000 found that cultural values have an influence on consumers' concerns about privacy. The same study, however, pointed out that there is a correlation between national regulation and privacy concerns: consumers coming from countries where there is a history of governmental regulation on personal data protection desire an even stronger regulation[48].

Also other previous empirical researches had demonstrated the same correlation between privacy perception and privacy policies. According to a research made in the late Nineties, related to information privacy corporate management and national regulation, "[a] country's cultural values are associated strongly with the privacy concerns that are exhibited by its populace". Furthermore, those values are associated, even if marginally, with the country's regulatory approach. Finally, the more individuals' privacy concerns rise, the more their demands for legal

[45] PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, cit., 49. The author criticizes this approach, claiming that it brought more problems than solutions. A more concrete example, even if outside the province of this work, would be the legislation of smoking in public places in Italy. The ban of the possibility to smoke in bars and offices has probably increased the consciousness of the dangers of cigarettes, as well as the social perception of smoking in public places as wrong and harmful for surrounding people. Undoubtedly, when the legislation was introduced, smoke was already perceived differently than it was some decades before, meaning: the majority of people had become aware of the negative effects of cigarettes. Social perception and policies reinforced each other in a virtuous scheme. This is in my view what has happened for information privacy in Italy. The same reasoning can be applied to USA; for some hints see D. KAHAN, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, 67 U. Chicago Law Rev. 607 (2000), 626-628.

[46] WHITMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, cit., 1160.

[47] In my research I just take these studies as they are, meaning that I do not question either the methods or the results. Nevertheless, each study includes a critical analysis of the methodology and of the limitations of the results.

[48] S. BELLMAN, E.J. JOHNSON, S.J. KOBRIN, G.L. LHOSE, *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, 20 The Information Society 313 (2004), 320.

intervention increase[49]. These findings suggest that when a country's regulation for privacy is perceived as inadequate, it is probable that pressures to increase governmental interventions occur[50].

Other studies reached slightly different conclusions. For example, an empirical research made in 1995 found that the level of personal information concern varies highly among countries. This seemed not to be linked to cultural values[51]. But at the same time there is a relation between cultural values of the population and privacy regulations of the country. Moreover, the more the population is concerned with privacy issues, the higher is the level of protection provided through regulation. The analysis revealed that "lower levels of information privacy concern [were] associated with "no regulation" countries and with the highest levels of government involvement in corporate privacy management, while higher levels of privacy concern [were] associated with more moderate regulatory structures"[52]. My understanding is that the intervention of a strong governmental regulation has led to a decrease of concern. The other side of the coin is that where no concern for privacy exists, there are no privacy regulation policies.

Finally, it is worth noting that, unlike what happens for copyright, privacy is not regulated by international treaties yet[53]. It emerged from the previous chapters that the biggest intervention at a supranational level is constituted by the OECD

[49] S.J. MILBERG, H.J. SMITH, S.J. BURKE, *Information Privacy: Corporate Management and National Regulation*, 11 Organization Science 35 (2000), 47. The research also found that "[t]here is also a marginal, positive association between the level of governmental involvement in corporate privacy management and re-spondents' preferences for strong laws", see *Ibidem*.

[50] MILBERG, SMITH, BURKE, *Information Privacy: Corporate Management and National Regulation*, cit., 48.

[51] S.J. MILBERG, S.J. BURKE, H.J. SMITH, E.A. KALLMAN, *Values, personal information privacy, and regulatory approach*, 38 Communications of the ACM 65 (1995), 70-71. However, the authors acknowledge that "the fact that some differences across countries were observed in [a] somewhat homogeneous population may suggest that more dramatic differences could be expected in a sample drawn from the general populations of the countries". In addition "the lack of support for the association between cultural values and information privacy concerns may be explained by the use of 1) a limited set of cultural values and 2) aggregate rather than individual value scores—constraints imposed by the survey's
length and the limitations of the surveyed organization"; cf. *Ibidem*, 72.

[52] MILBERG, BURKE, SMITH, KALLMAN, *Values, personal information privacy, and regulatory approach*, cit., 72.

[53] The role of international relations in the development of national privacy regulations is analysed by BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, cit., 130 ff. Unlike what I claim here, Bennett, whose work is dated 1992, wrote that "[t]he process of policy making in the data protection area is clearly one where broad transnational forces for convergence have transcended variations in national characteristics", cf. *Ibidem*, 150.

Guidelines. Even if the guidelines have been called "a fundamental statement of international consensus on communication policies"[54], they were not binding for the signatory states. This may be an expression of the lack of strong lobbies in favor of privacy protection. And this is also, unquestionably, a weak point of the whole regulation of privacy. In a globalized world like the one in which we live, the existence of a strong international position would be an incentive for a higher consideration of privacy even in national legislation.

The international aspect should not be underestimated with regard to the implementation of Canadian legislation on information privacy. European Directive 95/46 provided that personal data could be transferred to third countries only when they could grant an adequate level of protection for information privacy[55]. In order to continue trading transactions with EU, third countries have chosen either to adopt a new legislation or to negotiate with Europe for an agreement[56]. The former category includes Canada, while USA agreed with EU on the so called "Safe Harbor" privacy principles[57].

It can be concluded from the brief analysis made that, even if the right to privacy is a creature of the American system, Canada and Italy have been developing a more comprehensive, and therefore more protective, approach[58]. A number of different variables can play a more or less important role in policy making. There is no single reason which can give a sufficient explanation by itself. Factors affecting policy making diverge among countries, but also within the same country. The same factors can also change with time passing. This is clearly true also for the perception of privacy and the need for its protection. Therefore this element cannot itself be a

[54] Quotation from BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, cit., 138.
[55] Cf. Recitals n. 56 and 57, as well as arts. 25 and 26 of Directive 95/46.
[56] BELLMAN, JOHNSON, KOBRIN, LHOSE, *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, cit., 314. BENNETT, *Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, cit., analyzed the "emulation effect" in the implementation of privacy policies. See *Ibidem*, 123-128. The same Author also considered the convergence of regulation by "penetration". "The penetration process assumes that policy making by one country often entails implications and costs for others", see the same contribution at pages 140 ff.
[57] Follow the principles is the requirement for a US company in order to trade with European counterparts. The principles are: notice, choice, onward transfer, security, data integrity, access, and enforcement. For an brief overview see S. MERCADO KIERKEGAARD, *Safe Harbor Agreement: Boon or Bane?*, 1 Shidler J. L. Com. & Tech. 10 (2005), available at: http://www.lctjournal.washington.edu/vol1/a010Kierkegaard.html.
[58] According to RODOTÀ, *Repertorio di fine secolo*, cit., 212, the

sufficiently explanatory agent for the way the regulation of data protection was conceived by each state. However, it is highly probable that, among the factors at play, a correlation between the cultural perception for the protection of privacy and the way in which the considered systems regulate the issue exists.

Furthermore, given the influence of cultural feelings on privacy policies, it is my opinion that the same influence is exerted on judges in the case studies considered in this research. This happens both directly, since they live and are part of a particular society with its specific cultural sensitivities, and indirectly, as a consequence of the policies adopted by the state in which judges operate.

5.3 The perception and conception of copyright and file sharing in the three systems

I will now try to give some insights on the perception of copyright, with particular attention to file-sharing, considering at the same time the evolution of copyright policies in the digital technology era.

Starting right from policies, it should be first of all noted that intellectual property, and copyright in particular, are at the center of a number of international treaties. As mentioned in the previous chapter, this is in contrast with the approach to privacy in which, despite some supranational agreements and relations, there is no international treaty yet. The reason why I mention this difference at the beginning of my analysis is that the supranational intervention deeply affects national regulations. This can drift domestic policies away from national cultures and perceptions.

As seen in the previous chapters, to date the strongest approaches to the matter of copyright are the American and the Euro-Italian ones. Canada seems to have adopted a softer way, in which courts has interpreted copyright norms restrictively, as it emerges from the analysis of the cases[59]. USA and Italy show a continuous interest in copyright: in both countries the legislation has been constantly updated: while the structure in both copyright legislations has been maintained, many amendments have been introduced. This has been done to keep up with technological change, with the aim to protect copyright from the increasingly widespread

[59] In my analysis I am not referring to the "moral part" of copyright, but only to exploitation and economic rights.

violations enabled by new technologies. Thus, copyright province has been enlarged and now comprises many works which were not contemplated at the time the legislations were enacted. Also the number of different rights to which the copyright holder is entitled is nowadays higher.

For what file-sharing is concerned, both United States and Italy have modified the contents of their privacy legislations to adapt them to this new phenomenon. In both the systems, the unlawfulness of file-sharing is rather clearly stated. Furthermore, a part from the concrete modifications introduced in copyright regulation, a number of bills have been proposed, some of which very lately. Each bill tries to make regulation stricter, with the scope to contrast the so called copyright piracy. On the contrary, up to now, Canada has never enacted a regulation which expressly sanctions file-sharing. It is not by chance that it is the only system among those analyzed where a judge has wrote, even if between the lines, that file-sharing of copyrighted songs has to be considered legal[60].

In addition to this, it should be noted that intellectual property rights have been more and more often protected via technological tools, such as Digital Rights Management[61]. This is in contrast with the protection accorded to privacy, which has not succeeded in being defended through technology: indeed, privacy enhancing technologies are not as diffused as DRM systems for the protection of copyright. Privacy has been often left in care of soft law. Even if, as a prominent scholar has claimed, the protection of both these rights needs a complex mix of responses[62], the difference in the use of technology tells something about the importance given to protection of privacy[63]. The technological measures for the protection of copyright

[60] I am here referring to *BMG Canada Inc. v. John Doe*, [2004] 3 F.C.R. 241, for an analysis of which see supra, par. 3.4.

[61] On this issue see the already cited contribution by COHEN, *DRM and Privacy*, cit.; CAMERON, *Digital Rights Management: Where Copyright and Privacy Collide*, cit. See also the seminal book of L. LESSIG, *Code 2.0*, New York, 2006, available at http://codev2.cc/download+remix/Lessig-Codev2.pdf. For the European and Italian systems, see CASO (ed.), Digital rights management: *problemi teorici e prospettive applicative*, cit.; and CASO, Digital rights management: *il commercio delle informazioni digitali tra contratto e diritto d'autore*, cit. See also *Article 29 Data Protection Working Party* "Working document on data protection issues related to intellectual property rights", January 18, 2005, at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-8.

[62] LESSIG, *Code 2.0*, cit., 120 ff.

[63] Or about the lobbies of copyright! Cf. LESSIG, *Code 2.0*, cit., 200. See also LITMAN, *The Politics of Intellectual Property*, cit., 314, referring to organizations for public interests which, despite the intensive work, could never get "a seat at the table" of negotiations.

are themselves protected by rules such as those inside DMCA or Directive 2000/31. Again, Canada has up to now avoided the introduction of this type of regulation.

This difference finds its origin (also) in the Canadian delay in implementing the WIPO Treaties. In particular, the enforcement methods applied by USA and Italy are a precipitate of the implementation of the WIPO Treaties, through the DMCA and European Directive 2004/48. In contrast, Canada has not considered a specific instrument like the United States DMCA *subpoena* or the Italian 156*bis*, L. 633/41 yet. As seen, these two provisions seemed to provide a useful mechanism for copyright holders to obtain users' personal data in order to enforce their rights, whereas Canadian copyright holders have to rely on the "classical" tools supplied for the enforcement of any other private right[64].

These differences are probably going to disappear or at least lessen in the near future, given the possible adoption of Bill C-11 as an amendment to the Canadian Copyright Act. This is also true for a number of other tools protecting copyright, such as DRMs, TPMs and the illegality of their circumvention.

Differences could also be reduced when the so called ACTA agreement will come into force[65]. ACTA is the "Anti-Counterfeiting Trade Agreement between the European Union and its Member States", as well as with other countries among which there are Canada and the United States. The Agreement has been negotiated under secrecy for five years. Starting from Spring 2011, the Agreement has been opened for signature for two years.

The Agreement includes a number of provisions aiming at the protection of intellectual property rights and, more precisely, related to their enforcement. The Agreement asks the signatory states to "ensure that enforcement procedures are available under its law so as to permit effective action against any act of infringement of intellectual property rights covered by this Agreement, including

[64] Actually, from the analysis conducted in the previous chapters, it emerges that the DMCA *subpoena* as well as art. 156*bis*, L. 633/41 were not successful. In the former case, copyright holders had even to switch to the "classical" method of John Doe processes.

[65] I will here just quickly mention the Agreement, which can be found at http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf. Scholarly works on this issue are already countless; for an account of how ACTA was reached and of its contents, and for further bibliography see: C.R. MCMANIS, *The Proposed Anti-Counterfeiting Trade Agreement (ACTA): Two Tales of a Treaty*, 46 Hous. L. Rev. 1235 (2009); M. KAMINSKI, *Recent Development: The Origins and Potential Impact of the Anti-Counterfeiting Trade Agreement (ACTA)*, 34 Yale J. International L. 247 (2009). More recently: P.K. YU, *Six Secret (and Now Open) Fears of ACTA*, 64 S.M.U. L. Rev. 975 (2011).

expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements". Remedies shall be applied in a way that avoids the creation of barriers to legitimate trade. The Agreement states that "[p]rocedures adopted, maintained, or applied to implement the provisions […] shall be fair and equitable, and shall provide for the rights of all participants subject to such procedures to be appropriately protected". Furthermore "[i]n implementing the provisions of this Chapter, each Party shall take into account the need for *proportionality* between the seriousness of the infringement, the interests of third parties, and the applicable measures, remedies and penalties"[66].

The Agreement considers the possibility that the signatory Parties provide for criminal procedures and penalties to be applied for cases in which piracy is conducted on commercial scale and regards willful copyright or related rights. It should be regarded as "acts carried out on a commercial scale at least those carried out as commercial activities for direct or indirect economic or commercial advantage". More precisely the article asks the states to provide criminal remedies *at least* in the mentioned cases[67]. ACTA also provides that for these offenses penalties shall include imprisonment as well as monetary fines, which should be high enough to have a deterrent effect. Furthermore, in appropriate cases, these crimes shall be prosecuted *ex officio* by competent authorities[68].

For what is more strictly connected to the issue considered in this research, art. 11 seems to consider a discovery tool, such as those considered in the previous chapters. In fact, the provision states that "[w]ithout prejudice to its law governing privilege, the protection of confidentiality of information sources, or the *processing of personal data*, each Party shall provide that, in *civil judicial proceedings concerning the enforcement of intellectual property rights*, its judicial authorities have the authority, upon a justified request of the right holder, to order the infringer or, in the alternative, the alleged infringer, to provide to the right holder or to the judicial authorities, at least for the purpose of collecting evidence, relevant information as provided for in its applicable laws and regulations that the infringer or alleged infringer possesses or controls. *Such information may include information*

[66] All these quotations come from art. 6. Emphasis added.
[67] Cf. art. 23 of the Agreement. Emphasis added.
[68] See, respectively, arts. 24 and 26 of ACTA.

regarding any person involved in any aspect of the infringement or alleged infringement and regarding the means of production or the channels of distribution of the infringing or allegedly infringing goods or services, *including the identification of third persons* alleged to be involved in the production and distribution of such goods or services and of their channels of distribution"[69].

As mentioned, this article provides for a discovery tool which seems to me to be already in place in at least two of the three analyzed systems. The adoption of ACTA and its implementation would not change the current scenario for Italy and USA, where art. 156*bis* and DMCA *subpoena*, respectively, already comply with the ACTA requirements. On the contrary, Canada would probably need to implement a new tool, specifically dedicated to the enforcement of intellectual property.

As for the enforcement of intellectual property in the digital environment, art. 27 provides that each signatory state shall permit an effective action against an act of infringement of intellectual property which takes place on the digital environment. Section 4 of the same article provides that a signatory party "may provide, in accordance with its laws and regulations, its competent authorities with the authority to order an online service provider to *disclose* expeditiously to a right holder *information sufficient to identify a subscriber whose account was allegedly used for infringement,* where that right holder has filed a legally sufficient claim of […] copyright or related rights infringement, and where such information is being sought for the purpose of protecting or enforcing those rights. These procedures shall be implemented in a manner […] consistent with that Party's law, preserves fundamental principles such as freedom of expression, fair process, and *privacy*"[70].

This provision seems to complete the previous art. 11 and includes explicitly "information sufficient to identify a subscriber" into the category of information which can be asked and obtained by a copyright holder from a provider.

The reason why I have briefly exposed the most influential provisions of ACTA is that this is the latest of an increasing number of international treaties and agreements on intellectual property. The inclusion of a specific discovery tool for the cases of copyright infringement in the digital environment seems to aim at

[69] Emphasis added.
[70] Sections 5 and 6 of art. 27, concern remedies against the circumvention of technological measures protecting copyright.

overcoming the disparities among the different systems. Nonetheless, as already said, in my opinion at least two of the three countries analyzed do already include in their legislations a provision such as the one required by ACTA. Therefore I believe that the difference will be more in the way these instruments will be applied. Indeed, from the analysis of the previous chapters emerges that, despite similar tools, their application can vary greatly due to the different positions taken by judges. What I mean is that international policies are there and are implemented, but differences persist when they are applied.

Once illustrated copyright policies, I will now try to give an account of the perception of copyright.

The problem of public compliance with copyright and intellectual property laws was already in place in 1997[71], before the explosion of digital revolution. Empirical research underlined that the two most important factors influencing compliance with intellectual property law are morality and legitimacy. The former concerns an individual's personal feeling about what is right and what is wrong. The latter, instead, is related to one's feeling that one should obey the law. When these factors are there, voluntary compliance is promoted.

People do not consider uniformly lawbreaking as morally wrong: attitudes vary according to different types of illegal behavior. The findings on the scarce compliance with intellectual property law mean the lack of a public perception that breaking intellectual property law is wrong. Law can have a great symbolic function if it is in line with public views about what is fair, but it loses this power as the formal law departs from public morality[72]. In the opinion of the author of the research the key to reduce this discrepancy is to create a culture that supports intellectual property law[73].

The second factor is legitimacy. Legitimacy has a great advantage on morality: when something is perceived as legitimate, citizens obey the law even if

[71] T.R. TYLER, *Compliance with intellectual property laws: a psychological perspective*, 29 N.Y.U. Journal of International Law and Policy 219 (1997), 219.
[72] TYLER, *Compliance with intellectual property laws: a psychological perspective,* cit., 224-227, *passim*. The Author makes the example of "fair use": in his opinion the public seems to be operating within a sort of implicit standard of fair use, believing that some behaviors are acceptable while other are not. As Whitman notes "law will not work *as law* unless it seems to people to embody the basic commitments of their society"; cf. WHITMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, cit., 1220 (emphasis in original).
[73] TYLER, *Compliance with intellectual property laws: a psychological perspective,* cit., 229.

they do not feel that it is consistent with their personal morality. Legitimacy is closely related to the procedures through which legal authorities make rules. A central issue relates to the fairness of decision-making authorities, the so called "procedural justice". Together with fairness, another important characteristic is trustworthiness of legal authorities: when people feel that authorities are trying to be fair towards them, they are more willing to accept and obey rules[74].

With regard to our field of study, this argumentation would lead people to believe that intellectual property law (and copyright in our case) serves "reasonable social purposes and are not simply efforts to create profits for special interests groups, such as large corporation".

In the field of intellectual property there is the perception (better: the awareness) that laws respond to lobbies' interests in its greatest part[75]. It is sufficient to take into consideration the terms extension which the USA *Copyright Act* has been subjected. It is not by accident that the *Copyright Term Extension Act* of 1998 has been called "*The Mickey Mouse Protection Act*" due to the lobbying efforts made by Walt Disney company[76]. This is just an example related to the United States landscape. There is no reason to think that the same kind of mechanisms does not work also for the other two analyzed systems. This is actually confirmed by news and scholarly papers[77]. Up to now it seems that Canada is the most "lobby-proof"

[74] TYLER, *Compliance with intellectual property laws: a psychological perspective,* cit., 229-233, *passim*.

[75] In one sense this is probably true since the birth of copyright as we know it. See IZZO, *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico*, cit., *passim*. The entire book aims at explaining the interests behind the birth of copyright and *droit d'auteur*, which in the majority of cases were not authors' interests.

[76] Nor was the press unaware of this lobbying activities; see for example ASSOCIATED PRESS, *Disney Lobbying for Copyright Extension No Mickey Mouse Effort*, Chicago Tribune, October 17, 1998, at: http://homepages.law.asu.edu/~dkarjala/OpposingCopyrightExtension/commentary/ChiTrib10-17-98.html; and A.K. OTA, Disney In Washington: The Mouse That Roars, August 10, 1998, available at: http://edition.cnn.com/ALLPOLITICS/1998/08/10/cq/disney.html. This Act is just a single example of a consolidated practice, cf. J. LITMAN, *The Politics of Intellectual Property*, 27 Cardozo Arts & Entertainment Law J. 313 (2009), 314. More recently there was an objectional appointment of a previous RIAA's lobbist as federal judge: see N. ANDERSON, *RIAA lobbyist becomes federal judge, rules on file-sharing cases*, Astechnica.com, March 28, 2011, at: http://arstechnica.com/tech-policy/news/2011/03/riaa-lobbyist-becomes-federal-judge-rules-on-file-sharing-cases.ars.

[77] Just to give an example for the European landscape, see ERNESTO, *Music Industry Lobbyist Becomes Europe's Copyright Boss*, March, 31, 2011, at: http://torrentfreak.com/music-industry-lobbyist-becomes-europes-copyright-boss-110331/. See also M.K. RASMUSSEN, *Lobbying the European Parliament: A necessary evil*, Centre for European Policy Studies, May 2011, available at: www.ceps.eu/ceps/download/5533, especially at 3. For Canada, see the words of H. KNOPF, *Why Canadian Copyright Law I Already Stronger and Better Than That of The USA - and Why The USA*

among the three systems. This can be on of the reasons why, to date, Canada has the softest of the three analyzed copyright policies[78].

Furthermore, it should be noted that lobbies work also at a supranational level: by influencing international treaties lobbies are also able to influence national laws.

The existence of lobbies in the field of copyright is another big difference with the scenario of privacy protection. Copyright interests are powerful and organized in established organisms and institutions, while privacy interests are diffused and not organized. This is clearly on of the reasons why the technical and legislative regulation of copyright has been flourishing, whereas regulation was much less concentrated on solving privacy problems[79].

Going back to the perception of copyright, we can affirm that the well-known existence of lobbies influencing the creation of copyright legislation can be one of the factors leading people not to respect copyright. Indeed, according to procedural justice theory, if people perceive that copyright norms are shaped in great part in compliance with lobbies' interests, then they do not perceive these laws as fair and, therefore, they do not obey them. Since the presence and influence of lobbies is certain, it can be inferred that the mentioned effect is certain as well[80].

The author suggested that it was important investigating whether people felt the same way with regard to intellectual property infringement and to, for example, stealing software or videocassettes. The findings of this kind of research would help in understanding people's feelings on the legitimacy of legal authorities[81].

Should Look In The Mirror Rather Than At Its "Special 301" Watch List, 2008, 1, available at: http://fordhamipconference.com/wp-content/uploads/2010/08/Howard-Knof_canadian-copyright.pdf

[78] Again, as an example, see the questions posed by US copyright lobbies against the entrance of Canada in the "Trans-Pacific Partnership" (a free trade agreement that includes nations of both sides of the Pacific, which can be found at: http://fpc.state.gov/documents/organization/145583.pdf): M. GEIST, *US Copyright Lobby Wants Canada Out of TPP Until New Laws Passed, Warns of No Cultural Exceptions*, January 16, 2012, at: http://www.michaelgeist.ca/content/view/6243/125/.

[79] LESSIG, *Code 2.0*, cit., 200.

[80] Another point related to the fairness of copyright laws is that they do not favor the author, they rather favor recording companies. See the example posed by CIPPIC in its website, at http://www.cippic.ca/en/file-sharing#faq_is-file-sharing-legal. See also, again in the Canadian scenario, http://www.musiccreators.ca/wp/. "Canadian Music Creators' Coalition" was meant to be a coalition of Canadian authors whose aim was to have "[their] voices heard about the laws and policies that affect [their] livelihoods".

[81] Quotation and thoughts from TYLER, *Compliance with intellectual property laws: a psychological perspective,* cit., 233.

In fact, there are behaviors which are regarded as morally wrong by the vast majority of people, such as rape or murder, whereas there are behaviors which, even if formally punished by law, are not considered morally objectionable. "Social norms influence the creation and enforcement of law and are in turn influenced by the creation and enforcement of law"[82]. There is a so called "social norm" on file-sharing: "[s]ocial norms are the informal social and moral standards of a particular group which regulate the behavior of individuals within that group"[83]. What I am interested into is not whether copyright law will one day be totally respected or not, nor which strategies should be adopted in order to encourage compliance with copyright laws[84]. I am neither interested in why people follow these norms[85]. Instead, I am interested into the fact that there are social norms according to which copyright law infringement is *now* (and at the time of the analyzed lawsuits) considered socially acceptable.

In the last years a number of empirical studies have analyzed the perception of copyright, especially with regard to the digital environment. These researches spring from the awareness that file-sharing is not disappearing, despite the uninterrupted introduction of new laws and harsher sanctions, as well as despite the advertisement campaigns promoted by recording companies. It is not by chance that art. 31 of ACTA provides that "[e]ach Party shall, as appropriate, promote the adoption of measures to enhance public awareness of the importance of respecting intellectual property rights and the detrimental effects of intellectual property rights infringement".

---

[82] Words by SCHULTZ, *Copynorms: Copyright and Social Norms*, cit., 202.

[83] Quotation from G. NERI, *Sticky Fingers or Sticky Norms? Unauthorized Music Downloading and Unsettled Social Norms*, 93 Georgetown Law Journal 733 (2005), 746. In the last years social norms on copyright infringement have been studied widely. I will here just mention them in order to illustrate my point. For further bibliography see the contributions here cited.

[84] Many scholars have hypothesized different solutions for this problem; as an example see M.F. SCHULTZ, *Reconciling Social Norms and Copyright Law: Strategies for Persuading People to Pay for Recorded Music*, 17 Journal Intell. Prop. Law 59 (2009). C. JENSEN, *The More Things Change, the More They Stay the Same: Copyright, Digital Technology, and Social Norms*, 56 Stanford Law Review 531 (2003).

[85] For a brief account and further bibliography, see M.F. SCHULTZ, *Copynorms: Copyright and Social Norms*, in P.K. YU (ed.), *Intellectual Property and Information Wealth*, Westport, 2006, 206 ff. An appealing explanation is given by D.J. GERVAIS, *The Purpose of Copyright Law in Canada*, 2 University of Ottawa Law & Technology J. 315 (2005), 332 ff., available at: http://www.uoltj.ca/articles/vol2.2/2005.2.2.uoltj.Gervais.315-356.pdf. Prof. Gervais considers the history of copyright in different cultures and concludes that copyright was at the beginning meant as a moral right not to appropriate of someone else's work. "It [was] not the extraction of a payment for every drop of use of the work distilled to individual end-users", cf. *Ibidem*, 335.

A study conducted in 2004 among university students revealed that there is a different perception in the legality and ethic of copying a copyrighted software "traditionally" versus "via peer-to-peer"[86]. The majority of the participants in the survey considered "traditional" copying to be neither an illegal nor an unethical behavior[87]. This is already an indication on the perception of copyright laws. But moving to the exchange of copyrighted material via peer-to-peer, the vast majority (around two-thirds) of the students indicated that file-sharing was not illegal. Only a very small part of the participants indicated with certainty the illegal nature of file-sharing. The same results were reached with regard to the ethics of peer-to-peer. Finally, only a small percentage of respondents perceived that the activity was unethical (around 14%)[88].

An interesting point in this study is the comparison of file-sharing with shoplifting. In its advertisement campaigns the recording industry assimilates the two activities and tries to convince users that file-sharing is like stealing, like shoplifting[89]. The overwhelming majority of respondents indicated that they would not engage in shoplifting. And even more indicative is that 71% of respondent did not equate file-sharing activities through peer-to-peer networks to shoplifting copyrighted works in a retail store[90]. In my view this is a clear signal that there is no perception of file-sharing as a crime, which in turn means that copyright is not perceived in the same way than "classic" property is[91].

[86] R. MOORE, E.C. MCMULLAN, *Perceptions of peer-to-peer file sharing among university students*, 11 Journal of Criminal Justice and Popular Culture 1 (2004), available at: http://www.albany.edu/scj/jcjpc/vol11is1/moore.pdf. As in the previous paragraph, I will not question the validity of this and other surveys nor of their results.
[87] MOORE, MCMULLAN, *Perceptions of peer-to-peer file sharing among university students*, cit., 7.
[88] MOORE, MCMULLAN, *Perceptions of peer-to-peer file sharing among university students*, cit., 8-9.
[89] The most famous example is probably the spot showed in cinemas before the projection of movies: http://www.youtube.com/watch?v=HmZm8vNHBSU.
[90] MOORE, MCMULLAN, *Perceptions of peer-to-peer file sharing among university students*, cit., 8-10.
[91] The most intuitively explanation is the scarcity of "material" objects, which consumptions (or theft) deprives the owner of her goods. Whereas this is not true with regard to immaterial goods, such as those protected by intellectual property. MOORE, MCMULLAN, *Perceptions of peer-to-peer file sharing among university students*, cit., 13-14 give some different psychological explanations of the results of their study.

A more recent study conducted in the USA compared music download with music sharing (download plus upload) and shoplifting[92]. The study considered the correlation of the three mentioned activities with five different indicators:

- deterrence, which typical strategies are represented by the increase in the likelihood of being punished as well as by the increase of costs for engaging in illegal behavior;
- social influence, meant as mainly constituted by social norms; in this study, social norms are considered as the perceptions that the nearest persons, that is one's family and friends, have about committing illegal behavior;
- personal morality, which refers to the internalized obligation to obey the law;
- perceived legitimacy of authority. This is the external influence on compliance: in this sense it is opposite to personal morality. The more people believe that those in authority have a legitimate right to govern their behaviors, the more people obey the law. This study considered the opinion for the recording industry. In fact, even if the RIAA was not technically a legal authority, it nevertheless was the one which asked for enforcement;
- procedural justice, meaning the persons' perception of being treated fairly during the legal process[93].

As the previously mentioned study, also this one suggested that people view downloading and sharing music very differently from shoplifting. The above listed factors had a lesser influence on file-sharing behavior than on shoplifting, except for the perceived legitimacy of authority, which did not change between the two behaviors. As said, the most intuitive result of this research is that students see shoplifting and file-sharing as almost opposite situations. Students see this difference especially in terms of reasons to obey or not obey the law. Obligation to obey the law was highly correlated to compliance with laws. While the vast majority of surveyed students engaged in file-sharing activities, only few had ever shoplifted[94].

[92] T. WINGROVE, A.L. KORPAS, V. WEISZ, *Why were millions of people not obeying the law? Motivational influences on non-compliance with the law in the case of music piracy*, 17 Psychology, Crime & Law 261 (2011).
[93] WINGROVE, KORPAS, WEISZ, *Why were millions of people not obeying the law? Motivational influences on non-compliance with the law in the case of music piracy*, cit., 263-265.
[94] WINGROVE, KORPAS, WEISZ, *Why were millions of people not obeying the law? Motivational influences on non-compliance with the law in the case of music piracy*, cit., 271-273.

One of the most interesting findings of this study is that "there is an enormous support for the behavior within the internet community"[95]. Furthermore, the authors wrote that "[t]here may not be general public support, particularly among young people, for laws that penalize individuals for downloading and sharing digital music". They also suggest that new generation may never support this kind of laws, since they have grown up with this idea of "open access" to contents[96]. In my opinion, this could mean that in the future more and more people will not obey file-sharing laws, since with time passing every child will use the internet and its resources.

Backing further the results of these studies, one can look at the empirical, intuitive evidence represented by the existence of millions and millions of file-sharers. Every now and then the press publishes news regarding this widespread practice[97].

As I have argued for privacy, I believe that also for copyright the cultural perception of it and, even more, of file-sharing has an influence on judges' decisions. In this case, it seems that the perception is homogeneous in the three countries and that it actually goes beyond national borders. As mentioned in the first paragraph of this chapter, cultures are not necessarily national; indeed, there can be cultures

[95] WINGROVE, KORPAS, WEISZ, *Why were millions of people not obeying the law? Motivational influences on non-compliance with the law in the case of music piracy*, cit., 271.

[96] WINGROVE, KORPAS, WEISZ, *Why were millions of people not obeying the law? Motivational influences on non-compliance with the law in the case of music piracy*, cit., 274.

[97] Studies and related news are countless. I will here just make some examples, in order to support my point. As for Canada see ASSOCIATED PRESS, *Canada on U.S. copyright piracy watch list*, CBSnews.com, April 30, 2009 athttp://www.cbc.ca/news/technology/story/2009/04/30/copyright-piracy.html (telling how Canada was in the "watch list"; CIPPIC, How widespread is music file-sharing?, at http://www.cippic.ca/en/file-sharing#faq_how-widespread. See also on movie piracy: V. PILIECI, *Hollywood Blames Canada for Half of Movie Piracy,* Canada.com, Jan. 24, 2007, http://www.canada.com/topics/technology/story.html?id=f8ae08f5-b82d-4e87-97b9-67ff7097638f&k=65095. Italy shows a file-sharing rate which is among the highest of the world: cf. for example the table at: *Canada falls in online piracy ranking, CBSnews.com*, May 14, 2009, at http://www.cbc.ca/news/technology/story/2009/05/14/tech-090614-piracy-copyright-canada-baytsp.html (the article tells that Canada file-sharing rate decreased, while Italy places itself at the second place of the list of the highest "file-sharers" countries). For what USA are concerned, recent studies suggest that piracy rate has declined; nevertheless it remains at around 9% of the entire population (which is more than the people actually using the internet). Cf. L. GRAHAM, *With Limewire Shuttered, Peer-to-Peer Music File Sharing Declines Precipitously*, March 23, 2011, NPD.com, www.npd.com/press/releases/press_110323.html. See also *The Copy Culture Survey: Infringement and Enforcement in the US, November 15*, 2011, at http://piracy.ssrc.org/the-copy-culture-survey-infringement-and-enforcement-in-the-us/. The study this news makes reference to can be found at: http://piracy.ssrc.org/wp-content/uploads/2011/11/AA-Research-Note-Infringement-and-Enforcement-November-2011.pdf.

related to specific groups. In this case it would be probably correct to talk of an "internet-world-culture" or at least a "file-sharers' culture".

The studies analyzed here concentrate mainly on American society. Nevertheless, I believe that they can be generalized. The generalization is feasible due to some factors. As mentioned, file-sharing is a common practice in all the three considered systems. File-sharers are people which can be considered as a sort of single population, given the community in which they participate. Moreover, the three analyzed countries have similar characteristics in socio-economic terms. For these main reasons it can be inferred that the above illustrated empirical evidences equally apply to the USA, Canada and Italy.

So far I explained the factors which support the hypothesis for the existence of a widespread culture "against" copyright and, more precisely, against file-sharing. At the same time, I have also illustrated the different approaches taken by the three countries. Also due to the implementation of international treaties, Italy and United States seem to provide a wider and stronger protection for copyright than Canada does[98]. This is true even when we look at the case law[99]. It is not certain that the outlook will remain the same in the coming years: only time will provide the answer.

5.4 The tension under which judges are posed and the meaning of the adopted solutions

What I have been explaining so far is what I call the "perceptions and conceptions" of data protection and file-sharing in the three examined countries. I have also recalled the different solutions given by courts in the analyzed cases. It is now time to conclude my research and try to give an explanation for the different outcomes.

Once again, I wish to point out that my hypothesis is only a hypothesis. It does not pretend to encompass the whole complexity of variables which can play a

[98] For a different opinion see KNOPF, *Why Canadian Copyright Law I Already Stronger and Better Than That of The USA - and Why The USA Should Look In The Mirror Rather Than At Its "Special 301" Watch List*, cit., claiming: "Canada has always provided strong protection for creators and corporate copyright interests, and in very many important ways has done so for much longer and for much more principled reasons than the USA".

[99] GERVAIS, *The Purpose of Copyright Law in Canada*, cit., 356: "[Canadian] Supreme Court showed great reluctance in preventing use of copyright material by end-users".

role in the analyzed cases. My attempt is to give a possible explanation of the outcomes. It is clear that I do bear in mind the differences existing among the considered systems. As previously written, the simple fact that both USA and Canada have a common law tradition, whilst Italy has a civil law one, generates a lot of consequences which are left in the background of this thesis. Just to give a meaningful example let us consider the importance of *stare decisis* in the three countries. The role of judges has much greater importance in common law countries, than it has in countries like Italy. Many other more and less significant divergences persist, but they go beyond the scope of this work. I shall now try to support my hypothesis that judges solved the conflict between copyright enforcement and data protection in a way which is consistent with the "perceptions and conceptions" of the two rights in their countries.

To put it in a very simplistic way, the solutions adopted are the following: in the United States copyright won over privacy, while in the other two countries the opposite is true. I have argued in the previous paragraphs that United States and Italy have stronger copyright conception and perception than Canada, whereas, in terms of personal data protection, Italy and Canada show a more garantistic approach, than the one applied by USA.

As explained at the beginning of this chapter, in my view when (better: since) laws are ambiguous and allow different interpretations, judges can be influenced by the existing frameworks of the right at stake. In this sense they can both be affected by the overall policies applied in the country, as well as by the social or cultural attitude towards the right. I think this can offer an explanation why the cases on which this research concentrates reached such outcomes.

I believe that in the analyzed cases, courts found themselves caught in the middle. On one side there is policy. On the other side there is cultural perception. How can judges move from this impasse? I think that in the balancing, courts took into account both these things. This led to different solutions, as a result of the combination of policy and culture of the country in which they operate.

It should be noted that judges are, first of all "human being with the same cognitive machinery as everyone else"[100]. Indeed, many studies suggest that judges think and act as everyone: they are subject to the same cognitive biases of laypeople[101]. For this reason they are influenced by the society and culture of their country: to be more precise, they also participate in those culture and society. It is therefore possible that they follow the perception of that culture. This has been even hoped by some scholars[102]. Indeed, judges can perceive a predominant change in societal values which demand a reinterpretation of laws and rule accordingly[103].

As a prominent scholar has shown, the way in which decisionmakers, a category that undoubtedly comprises also judges, apply law depend also on the perception of the law itself: it depends on social norms. In particular he argues that when a social norm is particularly "sticky", decisionmakers are reluctant to apply a law whose intent is to modify that social norm[104]. In fact individuals are more willing to consider a conduct as worthy of condemnation when also the other people do the same. Therefore, when there are norms which are the result of lobbies activism, people will not consider them as representative of widespread consensus unless also their associates will[105]. Decisionmakers are influenced by society: when a social

[100] Quotation from C. GUTHRIE, J.J. RACHLINSKI, A.J. WISTRICH, *Blinking on the bench: how judges decide cases*, 93 Cornell Law R. 1 (2007), 13.
I realize that judges are not identical one to the other, even if are part of the same group. A part from the fact that every person is different from another, it is also true that judges differ for education and background, as well as for the way in which they are selected. Judges can be part of a first instance court, or an appeal one or even a supreme court. There are also judges which are part of a specialized section on a specific subject (such as intellectual property or tax law), and so on. Despite these divergences, I still think they can be grouped as a single category, given the tasks they need to carry out.
[101] See again GUTHRIE, RACHLINSKI, WISTRICH, *Blinking on the bench: how judges decide cases*. Many other experimental researches suggest the same conclusion; see for example C. GUTHRIE, J.J. RACHLINSKI, A.J. WISTRICH, *Inside the judicial mind*, 86 Cornell Law R. 777 (2001): "[the] study demonstrates that judges rely on the same cognitive decision-making process as laypersons", *Ibidem*, 829. See also the works collected in the volume edited by D. KLEIN, G. MITCHELL, *The Psychology of Judicial Decision Making*, New York, 2010. Another interesting book is L.S. WRIGHTSMAN, *Judicial Decision Making: Is Psychology Relevant?*, New York, 1999.
[102] GUTHRIE, RACHLINSKI, WISTRICH, *Blinking on the bench: how judges decide cases*, cit., make a summary of the most interesting and influential scholarly thought on this point.
[103] This seems it was the thought of Justice Cardozo, as mentioned by WRIGHTSMAN, *Judicial Decision Making: Is Psychology Relevant?*, cit., 47.
[104] I am referring to KAHAN, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, 67 U. Chicago Law Rev. 607 (2000).
[105] KAHAN, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, cit., 614. Evidently, this is deeply correlated with the theory of procedural justice.

norm has a widespread consensus, decisionmakers are reluctant to apply a new law which tries hard to modify the social norm[106].

It is plausible that this reasoning applies also to judges and, in particular, to judges enforcing copyright law. As seen, social norms are governing the phenomenon of file-sharing. At the same time there are laws which try to modify this norm. The attitude of some judges of not granting the order of disclosure could be the result of the mentioned reluctance to apply a law whose attempt is to modify a persistent social norm.

This can be the explanation for at least two of the three considered systems: I am referring to Canada and Italy. In these two countries social norms against copyright are probably more "sticky" than in the USA. This can be inferred, for example, by the number of file-sharers of each country. As seen, both these nations show high levels of piracy: hence, social norms relating to file-sharing are probably stronger than in USA.

We should also consider that, a part from the norms regulating copyright, in solving the conflict analyzed here perception and conception of privacy matter as well. As seen, Italian and Canadian approaches to this issue are more coherent and consistent; the defence of personal data protection is also stronger in both these systems than it is in the United States. This means that social perception of file sharing and data protection suggests the same solution to the conflict, meaning: not to disclose users' personal data. Therefore it was easier for judges to adopt this solution. This is true also for the Italian scenario: even if policy strongly protects copyright, the existence of both strong rules in favour of privacy and social norms for data protection (but against file-sharing punishment) suggests a clear solution against disclosure.

The situation of United States seems to be exactly the opposite. Social norms against file-sharing punishment are weaker than in the other two systems. The same is true for the perception and conception of personal data protection. If we add that copyright policies are probably the strongest among the three considered systems, it comes natural that copyright would prevail.

[106]KAHAN, *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, cit., 619-620.

Rules can be viewed as an instrument to reach certain goals and to implement certain values. When judges find themselves in the need to choose between two conflicting values, the preference goes to the rules that have a better impact on the value at stake. This is called "value-based priority". When a rule – in our case, a law – has a value impact which is better than the value impact of another rule, the former prevails on the latter[107].

Psychologists have claimed that when judges must decide cases where no law exists, they need to identify the best outcome of the dispute, which involves empirical observation, induction, and *moral reasoning*[108]. I believe that the cases here considered are somehow cases which are not governed by existing law. Psychologists affirm that when no law applies judges have to engage in moral reasoning, in order to understand how the state should response to the parties' dispute.

Scholars have conducted research in other fields of law, which support the view that the perception of population can influence the decisions taken by judges. For example, a study relating the adoption of children by same-sex couples, which was conducted analyzing a number of real decisions, suggests this conclusion. In that case, social perception (even if wrong) on gays and lesbians could influence judges' sentences due to the lack of objective standards on which courts should rely in deciding for adoption[109]. Clearly, children adoption is a more delicate question than the one here under scrutiny, let aside the fact that it is a completely different issue. Nevertheless, the study findings reinforce my view that norms that are not clearly defined, as those here analyzed, allow judges to be affected by cultural perceptions.

Even if there are no clear evidences that judges are influenced by the mainstream society's feelings, it cannot go unnoticed that judges are part of a given society. As already noted, "[j]ustice breathe the same air as their fellow citizens and they cannot divorce themselves from their sorroundings. Indeed, quite to the contrary, judges must perceive every movement, every poulse of society and be able

[107] SARTOR, *Legal Reasoning: A Cognitive Approach to the Law*, cit., 208-209.
[108] E. SHERWIN, *Features of Judicial Reasoning*, in D. KLEIN, G. MITCHELL (eds.), *The Psychology of Judicial Decision Making*, New York, 2010, 122. Emphasis added.
[109] T.E. LIN, *Social Norms and Judicial Decisionmaking: Examining the Role of Narratives in Same-Sex Adoption Cases*, 99 Columbia Law Review 739 (1999), spec. 769 ff.

to respond by moulding law, insofar as it is in their power, to the needs of their times"[110].

The reasoning on the way in which judges decided would make sense also if we looked only to what I have called the conception of the two rights. Indeed, in the Canadian context judges find themselves in front of a coherent and strong regulation of privacy and a weaker, even if consistent, protection of copyright. In Italy there is a solid and organic regulation of personal data, which is stronger than the one granted to copyright, also with reference to the constitutional protection enjoyed by privacy. Finally, as for United States judges face two completely different regulations: on the one side there is the strong and complete protection of copyright; on the other, personal data regulation is fragmented and incomplete.

Given these premises it is clear that when a judge is facing a conflict such as those here analyzed, it will give prevalence to the subject matter which is considered more important by the legal system as a whole.

The two arguments reinforce each other if we take into account the connection among the various factors. Policy is the result (also) of cultural and social perceptions. When judges face difficulties in finding a clear solution and need to apply general principles making reference to policies, they follow at the same time (also) cultural and social perceptions.

As far as I know, almost no scholar has investigated the possible influence of social attitudes on judicial decisions. The most part of works contributing to the issue of judges and culture or social norms consider the opposite relation, that is: whether judges can bring about a social change[111]. Conflicting solutions have been given to this question. I believe that, as very often happens, truth lies in the middle. Courts have the power to affect social perceptions, exactly in the way the legislator does. At the same time, courts can be the mouth through which common feelings can be given voice. I think this latter proposition applies to the cases I analyzed. Courts can bear the population's interests. But, in the mean time, if courts persist in rejecting the requests of copyright holders, they can give a signal which can affect and reinforce

[110] Quotation from J. DESCHÊNES, *The Judge as Lawmaker*, in A.M. LINDEN (ed.) *The Canadian Judiciary*, Toronto, 1976, 75.

[111] The literature on the issue is vast. As a mere example, and for further bibliography, take the seminal but controversial work of G. ROSENBERG, *The Hollow Hope: Can Courts Bring about SocialChange?*, Chicago, 1991.

social perception of copyright and data protection. To this extent we can say that there is a virtuous circle[112].

Now that the research draws to an end, one could wonder what is the meaning and what are the aims of this work. The research tries to offer a possible explanation for the approach taken in different countries for an identical problem. I am aware that it is a merely descriptive analysis. It has no pretension of explaining the whole mechanism of judicial decisions. Nor it is intended as a one-fits-all explanation, applicable to every judicial decision. It is neither meant as a prescriptive approach in which I suggest that judges should endorse cultural feelings.

I am aware of the limits of this analysis. I have deliberately left in the background a number of variables, in order to simplify my research, and somehow "isolate" my variable as social scientists do. Nonetheless, I think that this way of investigating could be interesting also for other kinds of lawsuits involving conflicting values[113]. I furthermore believe that legal scholars should enlarge their perspectives and embrace the knowledge of other disciplines, which can be of help for understanding of the "realm of law".

This is a case study whose aim was only to shed some light on the relation between society and judges, in those delicate cases where fundamental rights clash. To me, a better understanding of this phenomenon can help in the definition of a better law and, at the very end, of a better society. Indeed, "*[i]t is precisely this constant search for a balance between the fundamental rights of each individual which constitutes the foundation of a 'democratic society*'"[114].

[112] Or, again, a vicious one depending on the rules which will be reinforced.
[113] Let us for example think about cases of genetic patenting.
[114] ECHR, *Chassagnou v. France*, Applications nos. 25088/94, 28331/95 and 28443/95, April 29, 1999, par. 113. The sentence goes on as follows: "[t]he balancing of individual interests that may well be contradictory is a difficult matter, and Contracting States must have a broad margin of appreciation in this respect, since the national authorities are in principle better placed than the European Court to assess whether or not there is a "pressing social need" capable of justifying interference with one of the rights guaranteed by the [European Convention on Human Rights]".

Bigliography

AA.VV., *Microsoft Computer Dictionary*, Washington, 2002

ABRAMS L.S., MCGUINNES K.P., *Canadian Civil Procedure Law*, Markham, 2010

ABRIANI N., COTTINO G., RICOLFI M., *Diritto industriale*, in *Trattato di diritto commerciale diretto da Cottino*, Volume II, Padova, 2001

ALTMAN I., *Privacy Regulation: Culturally Universal or Culturally Specific?*, 33 Journal of Social Issues 66 (1977)

AMEDEO M., *Shifting the Burden: the Unconstitutionality of Section 512(h) of the Digital Millennium Copyright Act and its Impact on Internet Service Providers*, 11 CommLaw Conspectus 311 (2003)

ANDERSON N., *RIAA lobbyist becomes federal judge, rules on file-sharing cases*, Astechnica.com, March 28, 2011, at: http://arstechnica.com/tech-policy/news/2011/03/riaa-lobbyist-becomes-federal-judge-rules-on-file-sharing-cases.ars

ANDREPONT C., *Digital Millennium Copyright Act: Copyright Protection for the Digital Age*, 9 DePaul-LCA J. Art & Ent. L. 420, 412 ff. (1999)

ASHDOWN G.A., *Legitimate Expectation of Privacy*, 34 Vand. L. Rev. 1289 (1981)

ASSOCIATED PRESS, *Canada on U.S. copyright piracy watch list*, CBSnews.com, April 30, 2009 athttp://www.cbc.ca/news/technology/story/2009/04/30/copyright-piracy.html

ASSOCIATED PRESS, *Disney Lobbying for Copyright Extension No Mickey Mouse Effort*, Chicago Tribune, October 17, 1998, at http://homepages.law.asu.edu/~dkarjala/OpposingCopyrightExtension/commentary/ChiTrib10-17-98.html

ATELLI M., *Riservatezza (diritto alla). III) Diritto Costituzionale*, in *Enc. Giur. Treccani*, vol. XXVII, Roma, 1995

AUSTIN L.M., *Is Consent the Foundation of Fair Information Practices? Canada's Experience under Pipeda*, 56 University of Toronto L. J. 181 (2006)

AUTIERI P., *Il caso Napster alla luce del diritto comunitario*, in UBERTAZZI L.C. (ed.), *TV, Internet e «new trends» di diritti d'autore e connessi*, Milano, 2002, 63

BACKERMAN R., *Large Recording Companies v. the Defenseless – Some Common Sense Solution to the Challenges of the RIAA litigation*, 47 Judge J. 20 (2008)

BAILEY J., *The Substance of Procedure: Non-Party Disclosure in the Canadian and U.S. Online Music Sharing Litigation*, 43 Alta L. Rev. 615 (2006)

BALL H.G., *Law of Copyright and Literary Property*, New York, 1944

BANNERMAN S., *Copyright: Characteristics of Canadian Reform*, 16 in GEIST M. (ed.), *From "Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda*, Toronto, 2010, at

http://www.irwinlaw.com/store/product/666/from--radical-extremism--to--balanced-copyright-

BARNETT LIDSKY L., *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 Boston College L.R. 1373 (2009)

BARNETT LIDSKY L., *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 Duke L.J. 855 (2000)

BARNETT LIDSKY L., COTTER T., *Authorship, Ardencies, and Anonymous Speech*, 82 Notre Dame L. Rev. 1537 (2007).

BARRON J.A., DIENES C. T., *Constitutional Law in a Nutshell*, St Paul, 2005

BARTHEL T.J., RIAA v. Diamond Multimedia System, Inc.: *The Sale of The Rio Player Forces The Music Industry to Dance to a New Beat*, 9 DePaul-LCA J. Art & Ent. L. 279 (1999)

BASU D., *Obtaining disclosure from non parties*, 2 Journal of Personal Injury 198 (2005)

BEETS R.P., *RIAA v. Napster: The Struggle to Protect Copyrights in the Internet Age*, 18 Ga. St. U. L. Rev. 507 (2001)

BELLMAN S., JOHNSON E.J., KOBRIN S.J., LHOSE G.L., *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, 20 The Information Society 313 (2004)

BENNETT C.J.*, Regulating Privacy. Data Protection and Public Policy in Europe and the United States*, Ithaca (NY), 1992

BIANCA C.M., BUSNELLI F.D. (eds.), *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, Padova, 2007

BLACK H.C., *Black's Law Dictionary*, St Paul, 1979

BLACKMAN J.D., *Proposal For Federal Legislation Protecting Informational Privacy Across The Private Sector*, 9 Santa Clara Computer & High Tech. L. J. 431 (1993)

BLENGINO C., *La tutela penale del* copyright *digitale: un'onda confuse e asincrona*, in AA. VV., Copyright *digitale. L'impatto delle nuove tecnologie tra economia e diritto*, Torino, 2009, 69

BLENGINO C., SENOR M.A., *Il caso "Peppermint": il prevedibile contrasto tra protezione del diritto d'autore e tutela della* privacy *nelle reti* peer to-peer, in *Dir. inf. e informatica*, n. 4-5/2007, 835

BOAG J., *The Battle of Piracy versus Privacy: How the Recording Industry Association of America (RIAA) is Using the Digital Millennium Copyright Act (DMCA) As Its Weapon Against Internet Users' Privacy Rights*, 41 California Western Law Review 241, 243 (2004)

BOEVE M.R., *Will Internet Service Providers Be Forced to Turn In Their Copyright Infringing Customers? The Power of the Digital Millennium Copyright Act's Subpoena Provision After* In Re Charter Communication, 29 Hamline L.R. 177 (2006), at http://law.hamline.edu/files/vol29no1article6.pdf

BORLAND J.*, P2P users traveling by eDonkey*, CNET News.com, August 28, 2005, at http://news.cnet.com/P2P-users-traveling-by-eDonkey/2100-1025_3-5843859.html

BORLAND J., *Peer to peer: As the revolution recedes*, CNET News.com, December 31, 2001, at http://news.cnet.com/2100-1023-277478.html

BRADSHOW T., *Anonymous in revenge attack for MegaUpload shutdown*, Financial Times online, January 20, 2012, at http://blogs.ft.com/fttechhub/2012/01/anonymous-megaupload-ddos/#axzz1l2M8ZhJy

BRIDY A., *Why Pirates (Still) Won't Behave: Regulating P2P In The Decade After Napster*, 40 Rutgers Law J. 565 (2009)

BRIMSTED K., CHESNEY G., *The ECJ's judgement in Promusicae: The unintended consequences – music to the ears of copyright owners or a privacy headache for the future? A comment*, in 24 Computer Law & Security Report 275 (2008)

BUGIOLACCHI L., *La responsabilità dell'*host provider *alla luce del d.lgs. n. 70/2003: esegesi di una disciplina "dimezzata"*, in *Resp. civ. prev*., n. 1/2005

BUTTARELLI G., *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Milano, 1997

CALABRESI G., *The Costs of Accidents: A Legal and Economic Analysis*, New Haven, 1970

CALVERT C., GUTIERREZ K., KENNEDY K.D., CARNLEY MURRHEE K., *David Doe v. Goliath, Inc.: Judicial Ferment in 2009 for Business Plaintiffs Seeking the Identities of Anonymous Online Speakers*, 43 J. Marshall L. Rev. 1 (2009)

CAMERON A., CRTC *Imposes Super-PIPEDA Privacy Protection for Personal Information Collected by ISPs*, 10 I.E.C.L.C. 94 (2009)

CAMERON A., *Digital Rights Management: Where Copyright and Privacy Collide*, 2 Canadian Privacy Law R. 14, (2004)

CAMERON A., *Learning from data protection law at the nexus of copyright and privacy*, in KERR I. (ed.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society,* Oxford, 2009, 43

CARDARELLI F., SICA S., ZENO-ZENCOVICH V. (eds.), *Il codice dei dati personali: temi e problemi*, Milano, 2004

CARPAGNANO M., *Il* file-sharing *davanti alla corte suprema statunitense*, *Dir. Internet*, 2005, 568

CASO R. (ed.), Digital rights management*: problemi teorici e prospettive applicative*, Trento, 2008

CASO R., Digital Rights Management. *Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Padova, 2004

CASO R., *Il conflitto tra* copyright *e* privacy *nelle reti* Peer to Peer*: in margine al caso Peppermint – Profili di diritto comparato*, in *Dir. Internet*, n. 5/2007, 471, at

http://eprints.biblio.unitn.it/archive/00001334/01/Roberto_Caso.Peppermint_Copyright_Privacy_1_0_dicembre_2007.pdf

CASO R., *Il conflitto tra diritto d'autore e protezione dei dati personali: appunti dal fronte euro-italiano*, in *Dir. Internet*, n. 5/2008, 466, available at http://eprints.biblio.unitn.it/archive/00001637/

CASSANO G., CIMINO I.P., *Il nuovo regime di responsabilità dei* providers*: verso la creazione di un novello «censore telematico»*, in *Contratti*, n. 1/2004, 88

CERINA P., *Art. 2. Ambito di applicazione*, in GIANNANTONIO E., LOSANO M.G., ZENO ZENCOVICH V. (eds.), *La tutela dei dati personali. Commentario alla L. 675/1996*, Padova, 1999, 21

CHAFFEE-MCCLURE Z., *Train in Vain: The Clash Between the RIAA and the Eight Circuit over Whether the DMCA Subpoena Provision Applies to Peer-to-Peer Networks, and the Need to Steer the DMCA Back on Track with Congressional Intent* [*In re Charter Commc'ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771 (8th Cir. 2005)], 45 Washburn L.J 175 (2005)

CHARNETSKI W.A., FLAHERTY P.D., ROBINSON J.P., *The Personal Information Protection and Electronic Documents Act. A Comprehensive Guide*, Aurora, 2001

COHEN J.*, A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 Conn. Law Review 981 (1996)

COHEN J., *DRM and Privacy*, 18 Berkeley Tech. L.J. 575 (2003)

COLLIN S.M.H., *Dictionary of Computing*, London, 2004

COMANDÈ G., *Artt. 11 e 12 (Consenso – Casi di esclusione del consenso)*, in GIANNANTONIO E., LOSANO M.G., ZENO ZENCOVICH V. (eds.), *La tutela dei dati personali. Commentario alla L. 675/1996*, Padova, 1999, 114

CONSOLO C., *Spiegazioni di diritto processuale civile. Vol. I. Le tutele: di merito, sommarie ed esecutive*, Torino, 2010

COPELAND D., *SOPA, PIPA Votes Indefinitely Delayed*, readwriteweb.com, January 20, 2012, at: www.readwriteweb.com/archives/sopa_pipa_votes_indefinitely_delayed.php

COUDERT F., WERKERS E.*, In the Aftermath of the Promusicae Case: How to Strike the Balance?*, 18 International Journal of Law and Information Technology 50 (2008)

COX P., *Evolution or revolution? Norwich Pharmacal orders over the last 20 years*, Trademark World, 2004, 40, at http://www.sjberwin.com/Contents/Publications/pdf/102/220206124930.pdf

CRAIG C.J., *The Changing Face of Fair Dealing in Canadian Copyright Law: A Proposal for Legislative Reform*, in GEIST M. (ed.), *In The Public Interest: The Future of Canadian Copyright Law*, Toronto, 2005, 437

CUNEGATTI B., *Tutela amministrativa e giurisdizionale*, in MONDUCCI J., SARTOR G. (eds.), *Il codice in materia di protezione dei dati personali*, Padova, 2004, 487

D'AGOSTINI D., *Nessuna privacy per le persone giuridiche: le modifiche introdotte dal decreto "Salva Italia"*, CINDI – Centro innovazione e diritto, December 12,

2011, at http://associazionecindi.wordpress.com/2011/12/12/nessuna-privacy-per-le-persone-fisiche-le-modifiche-introdotte-dal-decreto-salva-italia/

D'AGOSTINI G., *Healing Fair Dealing? A Comparative Copyright Analysis of Canada's Fair Dealing to U.K. Fair Dealing and U.S. Fair Use*, 53 McGill L. J. 309 (2008)

D'ORAZIO R., *Art. 30. Istituzione del Garante*, in GIANNANTONIO E., LOSANO M.G., ZENO ZENCOVICH V. (eds.), *La tutela dei dati personali. Commentario alla L. 675/1996*, Padova, 1999, 397

DAINTITH J., WRIGHT E. (eds.), *A Dictionary of Computing*, Oxford, 2008

DAVID R., JAUFFRET-SPINOSI C., *I grandi sistemi giuridici contemporanei*, Padova, 1994

DE CATA M., *Il caso "Peppermint". Ulteriori riflessioni anche alla luce del caso "Promusicae"*, in *Riv. dir. industirale*, n. 4-5/2008, 404

DE CATA M., *La responsabilità civile dell'Internet* service provider, Milano, 2010

DELCHIN R.J., *Musical Copyright Law: Past, Present and Future of Online Music Distribution*, 22 Cardozo Arts & Ent. L.J. 343 (2004)

DESCHÊNES J., *The Judge as Lawmaker*, in LINDEN A.M. (ed.) *The Canadian Judiciary*, Toronto, 1976, 57

DI AMATO A., *Musica* on-line *e tutela penale*, in *Dir. Internet*, n. 4/2007, 329

DI FEDERICO G. (ed.), *Ordinamento giudiziario. Uffici giudiziari, CSM e governo della magistratura*, Padova, 2008

DI MICO L., *Il rapporto tra diritto di autore e diritto alla riservatezza: recenti sviluppi nella giurisprudenza comunitaria*, in *Il diritto di autore*, n. 1/2010, 1

DRASSINOWER A., *CCH Canadian Limited v. The Law Society Of Upper Canada: A Primer*, 28 Canadian Law Libraries 201 (2003)

DUTCHER T.A., *A Discussion of the Mechanics of the DMCA Safe Harbor and Subpoena Power, as Applied in* RIAA v. Verizon Internet Services, 21 Santa Clara Computer & High Tech. L.J. 493 (2005)

EFF, *Recording Industry Announces Lawsuits Against Music Sharers*, 2003, at http://w2.eff.org/IP/P2P/20030908_eff_pr.php

EFF, *RIAA v. The People: Four Years Later*, 2007, at http://w2.eff.org/IP/P2P/riaa_at_four.pdf

EFF, *Why the RIAA's "Amnesty" Offer is a Sham*, 2004, http://w2.eff.org/share/amnesty.php

ERNESTO, *Music Industry Lobbyist Becomes Europe's Copyright Boss*, March, 31, 2011, at http://torrentfreak.com/music-industry-lobbyist-becomes-europes-copyright-boss-110331/

ESMAIL P., CCH Canadian Ltd v. Law Society of Upper Canada: *Case Comment on a Landmark Copyright Case*, 10 Appeal 13 (2005)

FABIANI M., *Il caso M.G.M. contro Grokster, ovvero della responsabilità per l'altrui indebito utilizzo di opere protette*, *Dir. Autore*, 2006, 14

FEWER D., *Making Available: Existential Inquiries*, in GEIST M. (ed.), *In the Public Interest: the Future of Canadian Copyright Law*, Toronto, 2005, at http://www.irwinlaw.com/pages/in-the-public-interest--the-future-of-canadian-copyright-law

FICI A., PELLECCHIA E., *Il consenso al trattamento*, in PARDOLESI R. (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, Milano, 2003, 469

FICSOR M., *The law of copyright and the Internet: the 1996 WIPO treaties, their interpretation, and implementation*, Oxford, 2002

FINOCCHIARO G., *Anonymity and the law in Italy*, in KERR I., STEEVES V., LUCOCK C. (eds.), *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York, 2009, 523

FLAHERTY D.H., *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 Case W. Res. L. Rev. 831 (1991)

FLAHERTY D.H., *Protecting Privacy in Surveillance Society. The Federal Republic of Germany, Sweden, France, Canada & the United States*, Chapel Hill, 1989

FLAHERTY D.H., *Reflection on Reform of Federal* Privacy Act, Publications of the Office of the Privacy Commissioner of Canada, 2008, at http://www.priv.gc.ca/information/pub/pa_ref_df_e.cfm

FLAHERTY D.H., *The need for an American privacy protection commission*, 1 Government Information Quarterly 235 (1984)

FLOR R., *Tutela penale ed autotutela tecnologica dei diritti d'autore nell'epoca di internet. Un'indagine comparata in prospettiva europea ed internazionale*, Padova, 2010

FOGARTY P., *Major Record Labels and The RIAA: Dinosaurs in a Digital Age?*, 9 Hous. Bus. & Tax L.J. 140, 170 ff. (2008)

FOGLIA G., *La* privacy *vale più del diritto d'autore: note in materia di* filesharing *e di sistemi* peer-to-peer, in *Dir. industriale*, n. 6/2007, 585

FOX A.R., *The Digital Millennium Copyright Act: Disabusing the Notion of a Constitutional Moment*, 27 Rutgers Computer & Tech. L.J. 267 (2001)

FREER R.D., *Civil Procedure*, New York, 2009

FRIEDENTHAL J.H., KANE M.K., MILLER A.R., *Civil Procedure*, St Paul, 2005

FROOMKIN M., *Anonymity and the Law in the United States*, in KERR I., STEEVES V., LUCOCK C. (eds.), *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, New York, 2009, 441

GAMBARO A., SACCO R., *Sistemi giuridici comparati*, Torino, 2008

GAMBINI M., *Diritto d'autore e tutela dei dati personali: una difficile convivenza in Rete*, in *Giur. it.*, n. 2/2009, 509

GAMBINI M., *Le responsabilità dell'Internet* service provider, Napoli, 2006

GARDINI G., *Le regole dell'informazione. Principi giuridici, strumenti, casi*, Milano, 2005

GARZIA M.A., *Art. 24. Casi nei quali può essere effettuato il trattamento senza consenso*, in BIANCA C.M., BUSNELLI F.D. (eds.), *La protezione dei dati personali: commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, Padova, 2007, 558

GEIST M., *Copyright Is Back: Why Canada is Keeping the Flawed Digital Lock Rules*, September 29, 2011 at http://www.michaelgeist.ca/content/view/6033/125/

GEIST M., *Hurt Locker File Sharing Suits Come North: Federal Court Orders ISPs to Disclose Subscriber Info*, September 9, 2011, at http://www.michaelgeist.ca/content/view/5999/125/

GEIST M., *Internet Law in Canada*, Concord, 2002

GEIST M., *US Copyright Lobby Wants Canada Out of TPP Until New Laws Passed, Warns of No Cultural Exceptions*, January 16, 2012, at http://www.michaelgeist.ca/content/view/6243/125/

GELLMAN R., *An American privacy protection commission: an idea whose time has come…again*, 11 Government Information Quarterly 245 (1994)

GERVAIS D.J., *A Uniquely Canadian Institution: the Copyright Board of Canada*, in GENDREAU Y. (ed.), *Emerging Intellectual Property Paradigm: Perspectives from Canada*, Cheltenham, 2008, 197

GERVAIS D.J., *Application Of An Extended Collective Licensing Regime In Canada: Principles And Issues Related To Implementation*, Study Prepared for the Department of Canadian Heritage, 2003, at http://aix1.uottawa.ca/~dgervais/publications/extended_licensing.pdf

GERVAIS D.J., *Canadian Copyright Law Post-CCH*, 18 Intellectual Property Journal 131 (2004)

GERVAIS D.J., *The Price of Social Norms: Towards a Liability Regime for File-Sharing*, 12 J. Intell. Prop. Law 39, 55 ff. (2004)

GERVAIS, *The Purpose of Copyright Law in Canada*, 2 University of Ottawa Law & Technology J. 315 (2005), at: http://www.uoltj.ca/articles/vol2.2/2005.2.2.uoltj.Gervais.315-356.pdf

GIANNACCARI A., *L'ambito di applicazione della legge, l'importazione e l'esportazione dei dati personali*, in PARDOLESI R. (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, Milano, 2003, 142

GIANNANTONIO E., LOSANO M.G., ZENO ZENCOVICH V. (eds.), *La tutela dei dati personali. Commentario alla L. 675/1996*, Padova, 1999

GINSBURG J., T*he (New?) Right Of Making Available To The Public*, 234 in VAVER D., BENTLY L. (eds.), *Intellectual Property in the New Millennium, Essays in Honour of William R. Cornish*, Cambridge, 2004

GLEICHER N., *John Doe Subpoenas: Toward a Consistent Legal Standard*, 118 Yale L. J. 320 (2008)

GOHRING N., *Anonymous Retaliates for Megaupload Shutdown, Attacks DOJ, Others*, Pcworld.com, January 20, 2012, at http://www.pcworld.com/businesscenter/article/248445/anonymous_retaliates_for_megaupload_shutdown_attacks_doj_others.html

GORINI S., NIGER S., *Privacy e comunicazioni elettroniche*, in MONDUCCI J., SARTOR G. (eds.), *Il codice in materia di protezione dei dati personali*, Padova, 2004, 387

GORSKI D., *The Future of the Digital Millennium Copyright Act (DMCA) Subpoena Power on the Internet in Light of* Verizon Cases, 24 Rev. Litig. 149 (2005)

GOSSE E.R., Recording Industry Association of America v. Diamond Multimedia System, Inc.: *The RIAA could not stop the Rio-MP3 Files and the Audio Home Recording Act*, 34 U.S.F. L. Rev. 575 (1999)

GRAHAM L., *With Limewire Shuttered, Peer-to-Peer Music File Sharing Declines Precipitously*, March 23, 2011, NPD.com, www.npd.com/press/releases/press_110323.html

GRANIERI M., *Il sistema della tutela diritti nella legge 675/1996*, in PARDOLESI R. (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 2, Milano, 2003, 437

GRECO P., VERCELLONE P., *I diritti sulle opere dell'ingegno*, in *Trattato di diritto civile italiano redatto da diversi giureconsulti sotto la direzione di Filippo Vassalli*, Torino, 1974

GROSSO A., *Legally speaking: the promise and problems of the No Electronic Theft Act*, 43 Communications of the ACM 23 (2000)

GROUSSOT X., *Rock the KaZaA: Another Clash of Fundamental Rights*, 45 Common Market Law Review 1745 (2008)

GUTHRIE C., RACHLINSKI J.J., WISTRICH A.J., *Blinking on the bench: how judges decide cases*, 93 Cornell Law R. 1 (2007)

GUTHRIE C., RACHLINSKI J.J., WISTRICH A.J., *Inside the judicial mind*, 86 Cornell Law R. 777 (2001)

HAGEN G.R., ENGFIELD N., *Canadian Copyright Reform: P2P Sharing, Making Available and the Three-Step Test*, 3 UOLTJ 477 (2006)

HALPERN S.E., *New Protections for Internet Service Providers: An Analysis of "The Online Copyright Infringement Liability Limitation Act"*, 23 Seton Hall Legis. J. 359 (1999)

HALPERN S.W., *Copyright Law: Protection of Original Expression*, Durham, 2010

HALPERN S.W., NARD C.A., PORT K.L., *Fundamentals of United States Intellectual Property Law: Copyright, Patent, Trademark*, Alphen aan den Rijn, 2011

HANDA S., *Copyright Law in Canada*, Markham, 2002

HAYES M.S., *The Impact of Privacy on Intellectual Property in Canada*, 20 Intellectual Property Journal 67 (2006)

HAYHURST W.L., *The Canadian Supreme Court On Copyright*: CCH Canadian Ltd. v. Law Society Of Upper Canada, 41 Can. Bus. L.J. 134 (2004)

HOGG P.W., *Constitutional Law of Canada*, Toronto, 2010

HOLLANDER C., *Norwich Pharmacal takes wings*, 28 Civil Justice Quarterly 458 (2009)

HUMPHREY J.S., *Recent Development: Debating the Proposed Peer-to-Peer Piracy Prevention Act: Should Copyright Owners be Permitted to Disrupt Illegal File Trading Over Peer-to-Peer Networks?*, 4 North Carolina J. of Law & Technology 375 (2003)

IMFELD C., SMITH EKSTRAND V., *The Music Industry and the Legislative Development of the Digital Millennium Copyright Act's Online Service Provider Provision*, 10 Comm. L. & Pol'y 291 (2005)

INSTITUTE FOR INFORMATION LAW, *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems*, Amsterdam, 1998, at http://www.ivir.nl/publications/koelman/privreportdef.pdf

IZZO U., *Alle origini del copyright e del diritto d'autore. Tecnologia, interessi e cambiamento giuridico*, Roma, 2010

JENSEN C., *The More Things Change, the More They Stay the Same: Copyright, Digital Technology, and Social Norms*, 56 Stanford Law Review 531 (2003)

JONES J.D., *Cybersmears and John Doe: How Far Should First Amendment Protection of Anonymous Internet Speakers Extend?*, 7 First Amend. L. Rev. 421 (2009)

JUDGE E.F., GERVAIS D.J., *Intellectual Property: The Law in Canada*, Toronto, 2011

KADISH H.S., *The Crisis of Overcriminalization*, 374 *The Annals of the American Academy of Political and Social Science* 157 (1967)

KAHAN D., *Gentle Nudges vs. Hard Shoves: Solving the Sticky Norms Problem*, 67 U. Chicago Law Rev. 607 (2000)

KAMINSKI M., *Recent Development: The Origins and Potential Impact of the Anti-Counterfeiting Trade Agreement (ACTA)*, 34 Yale J. International L. 247 (2009).

KAO A., *RIAA v. Verizon: Applying the Subpoena Provision of the DMCA*, 19 Berkeley Tech. L.J. 405 (2004)

KATYAL S.K., *Privacy v. Piracy*, 7 Yale J. Law & Tech. 222 (2004)

KERR I., CAMERON A., *Nymity, P2P & ISPs: Lessons from BMG Canada Inc. v. John Doe*, in STANDBURG K.J., STAN RAICU D. (eds.), *Privacy and Technologies of Identity: a Cross Disciplinary Conversation*, New York, 2006, 269

KERR I., *The Legal Relationship Between Online Service Providers and Users*, 35 Can. Bus. L.J. 419 (2001)

KIERKEGAARD S., *ECJ rules on ISP disclosure of subscribers' personal data in civil copyright cases – Productores de Música de España (Promusicae) v Telefónica de España SAU (Case C-275/06)*, in 24 Computer Law & Security Report 268 (2008)

KLEIN D., MITCHELL G. (eds.), *The Psychology of Judicial Decision Making*, New York, 2010

KNOPF H., *Why Canadian Copyright Law I Already Stronger and Better Than That of The USA - and Why The USA Should Look In The Mirror Rather Than At Its "Special 301" Watch List*, 2008, available at: http://fordhamipconference.com/wp-content/uploads/2010/08/Howard-Knof_canadian-copyright.pdf

KOŠČÍK M., *Privacy Issues In Online Service Users' Details Disclosure In The Recent Case-Law. Analysis of Cases Youtube v. Viacom and Promusicae vs. Telefonica*, 3 Masaryk U. J.L. & Tech. 259 (2009)

KRONMAN A.T., *The privacy exemption to the Freedom of Information Act*, 9 J. Legal Studies 731 (1980)

KUNER C., *Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice*, 5 European Intellectual Property Review 199 (2008)

LAFRANCE M., *Copyright Law in a Nutshell*, St Paul, 2008

LAMBO L., *La disciplina sul trattamento dei dati personali: profili esegetici e comparatistici delle definizioni*, in PARDOLESI R. (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, Milano, 2003, 59

LANE F.S., *American Privacy. The 400-Year History of Our Most Contested Right*, Boston, 2010

LAROCHE K., PRATTE G.J., *The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation*, 18 Canadian Intellectual Property Review 117, 119 (2001).

LATTANZI R., *Protezione dei dati personali e diritti di proprietà intellettuale: alla ricerca di un difficile equilibrio*, in *Jus*, n. 1-2/2005, 233

LESSIG L., *Code 2.0*, New York, 2006, at http://codev2.cc/download+remix/Lessig-Codev2.pdf

LEVIN A., NICHOLSON M.J., *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 University of Ottawa Law & Tech. J. 357 (2005)

LEVIN D.R., *The Future of Copyright Infringement:* Metro-Goldwyn-Mayer Studios, Inc., v. Grokster, Ltd., 21 St. John's J. Legal Comment. 271 (2006)

LIBEU A., *What is a reasonable expectation of privacy?*, 12 W. St. U. L. Rev. 849 (1985)

LIN T.E., *Social Norms and Judicial Decisionmaking: Examining the Role of Narratives in Same-Sex Adoption Cases*, 99 Columbia Law Review 739 (1999)

LIPKUS N., *A Tale of Two Remedies: Rationalizing the Anton Piller Order in Canada*, 19 Intellectual Property Journal 459 (2006)

LITMAN J., *Copyright and Personal Copying: Sony v. Universal City Studios Twenty-One Years Later*, 55 Case W. Res. 917 (2005).

LITMAN J., *The Politics of Intellectual Property*, 27 Cardozo Arts & Entertainment Law J. 313 (2009)

LITMAN J., *The story of Sony v. Universal Studios: Mary Poppins Meets the Boston Strangler (Copyright)*, in GINSBURG J.C., DREYFUSS R.C., *Intellectual Property Stories*, New York, 2006, 358

MANDRIOLI C., *Corso di diritto processuale civile*, Editio minor, vol. III, Torino, 2011

MANTELERO A., *L'idea del* peer to peer *fra tutela della privacy ed* enforcement *dei diritti d'autore*, in *Riv. trim. dir. e proc. civile*, n. 4/2008, 1481

MARCHETTI P., UBERTAZZI L.C., *Commentario breve alla leggi su proprietà intellettuale e concorrenza*, Padova, 2007,

MARSHALL D.S., *First Impressions of a Troubling Case: Some Comments on* CCH Canadian Limited V. The Law Society Of Upper Canada, 25 Canadian Law Libraries 19 (2000)

MARUCCIA A., *Logistep, fine dei giochi. In Svizzera*, Punto-informatico.it, September 10, 2010, at http://punto-informatico.it/2987767/PI/News/logistep-fine-dei-giochi-svizzera.aspx

MARZANO P., *Diritto d'autore e* digital technologies. *Il* digital copyright *nei trattati OMPI, nel DMCA e nella normativa comunitaria*, Milano, 2005

MASSEY C., *American Constitutional Law: Powers and Liberties*, New York, 2001

MASSIMINI A., *Cyberdiritto d'autore*, Napoli, 1999

MAZZOTTA M., *Balancing Act: Finding Consensus On Standards For Unmasking Anonymous Internet Speakers*, 51 Boston College L.R. 833 (2010)

MCCARTHY C., *File-sharing site eDonkey kicks it, CNET News.com*, September 13, 2006, at http://news.cnet.com/File-sharing-site-eDonkey-kicks-it/2100-1030_3-6115353.html

MCCULLAGH D., *'Pirate Act' raises civil rights concerns*, CNETNews.com, May 26, 2004 at http://news.cnet.com/'Pirate-Act'-raises-civil-rights-concerns/2100-1027_3-5220480.html

MCGILL D.A., *New Year, New Catch-22: Why the RIAA's Proposed Partnership with ISPs Will Not Significantly Decrease The Prevalence of p2p Music File Sharing*, 29 Loy. L.A. Ent. L. Rev. 353 (2009)

MCISAAC B., SHIELDS R., KLEIN K., *The law of privacy in Canada*, Toronto, 2007

MCKEOWN J.S., *Fox on Canadian Law of Copyright and Industrial Designs*, Scarborough, 2000

MCMANIS C.R., *The Proposed Anti-Counterfeiting Trade Agreement (ACTA): Two Tales of a Treaty*, 46 Hous. L. Rev. 1235 (2009)

MCNAIRN C.H.H., *A Guide to the Personal Information Protection and Electronic Documents Act*, Markham, 2010

MCNAIRN C.H.H., SCOTT A.K., *Privacy Law in Canada*, Markham, 2001

MERCADO KIERKEGAARD S., *Safe Harbor Agreement: Boon or Bane?*, 1 Shidler J. L. Com. & Tech. 10 (2005), at http://www.lctjournal.washington.edu/vol1/a010Kierkegaard.html

MERGES R.P., GINSBURG J.G., *Foundations of Intellectual Property*, New York, 2004

MERGES R.P., MENELL P.S., LEMLEY M.A., *Intellectual Property in the New Technological Age*, New York, 2010

METZGER M.J., DOCTER S., *Public Opinion and Policy Initiatives for Online Privacy Protection*, 47 J. Broad. & Elec. Media 350 (2003)

MILBERG S.J., BURKE S.J., SMITH H.J., KALLMAN E.A., *Values, personal information privacy, and regulatory approach*, 38 Communications of the ACM 65 (1995)

MILBERG S.J., SMITH H.J., BURKE S.J., *Information Privacy: Corporate Management and National Regulation*, 11 Organization Science 35 (2000)

MIN CHEE-FONG A., *Unmasking the John Does of Cyberspace: Surveillance by Private Copyright Owners*, 4 CJLT 169 (2005)

MITCHELL J., *Wikipedia: So How Do You Like Censorship?*, readwriteweb.com, January 19, 2012, at: http://www.readwriteweb.com/archives/wikipedia_so_how_do_you_like_censorship.php

MONDUCCI J., SARTOR G. (eds.), *Il codice in materia di protezione dei dati personali*, Padova, 2004

MONTESQUIEU C.L., *Œuvres complètes de Montesquieu: avec des notes de Dupin, Crevier, Voltaire, Mably, Servan, La Harpe*, Livre XI, Chapitre VI, Paris, 1838

MOORE R., MCMULLAN E.C., *Perceptions of peer-to-peer file sharing among university students*, 11 Journal of Criminal Justice and Popular Culture 1 (2004), available at http://www.albany.edu/scj/jcjpc/vol11is1/moore.pdf

MORTON F.L. (ed.), *Law, politics and the judicial process in Canada*, Calgary, 2002

MURRAY L., *Copyright Talk: Patterns and Pitfalls in Canadian Policy Discourses*, in GEIST M. (ed.), *In the Public Interest: the Future of Canadian Copyright Law*, Toronto, 2005, 15

NELKEN D., *Using the concept of legal culture*, 29 Australian journal of legal philosophy 1 (2004)

NERI G., *Sticky Fingers or Sticky Norms? Unauthorized Music Downloading and Unsettled Social Norms*, 93 Georgetown Law Journal 733 (2005)

NETANEL N.W., *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 Harv. J.L. & Tech. 1 (2003)

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006

NIGER S:, *Il diritto alla protezione dei dati personali*, in MONDUCCI J., SARTOR G. (eds.), *Il codice in materia di protezione dei dati personali*, Padova, 2004, 1

NIMMER D., *A tale of Two Treaties*, 22 Colum.-VLA J.L. & Arts 1 (1997)

NIMMER D., *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 Cardozo L. Rev. 917 (2002)

NIMMER D., *Copyright: Sacred Test, Technology, and the DMCA*, The Hague, 2003

NISSENBAUM H., *Privacy in Context. Technology, Policy, and the Intergity of Social Life*, Standford, 2010

O'FLYNN T., *File sharing: an holistic approach to the problem*, 17 Entertainment Law Review 218 (2006)

O'HARE J., BROWNE K., *Civil litigation*, London, 2009

OTA A.K., Disney In Washington: The Mouse That Roars, August 10, 1998, available at http://edition.cnn.com/ALLPOLITICS/1998/08/10/cq/disney.html

PALLARO P., *La privacy nel settore delle telecomunicazioni: la direttiva comunitaria n. 97/66*, in *Riv. dir. europeo*, n. 3/1998, 541

PALMIERI A., *DRM e disciplina europea della protezione dei dati personali*, in CASO R. (ed.), *Digital rights management: problemi teorici e prospettive applicative*, Trento, 2008

PARDOLESI R. (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003

PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in PARDOLESI R. (ed.), *Diritto alla riservatezza e circolazione dei dati personali*, vol. 1, Milano, 2003, 1

PASCUZZI G., *Il diritto dell'era digitale*, Bologna, 2010

PASCUZZI G., *La videoregistrazione domestica di opere protette davanti alla "Supreme Court"*, in *Foro it*., 1984, IV, 351

PASCUZZI G., *Opera musicali su Internet: il formato MP3*, in *Foro it*., 2001, IV, 101

PASCUZZI G., *Videoregistrazione e "copyright" statunitense: violazione, "fair use" o terza via?*, in *Foro it*., 1984, IV, 23

PASETTI G., *Il garante per la protezione dei dati personali*, in MONDUCCI J., SARTOR G. (eds.), *Il codice in materia di protezione dei dati personali*, Padova, 2004, 513

PATRY W.F., *The fair use privilege in copyright law*, Washington, 1995

PATTI S., *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civile*, n. 4/99, II, 455

PEGUERA M., *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 Columbia Journal of Law & the Arts 481, 2009

PERRIN S., BLACK H.H., FLAHERTY D.H., MURRAY RANKIN T., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, Toronto, 2001

PILIECI V., *Hollywood Blames Canada for Half of Movie Piracy,* Canada.com, Jan. 24, 2007, http://www.canada.com/topics/technology/story.html?id=f8ae08f5-b82d-4e87-97b9-67ff7097638f&k=65095

POUND R., *The need of a sociological jurisprudence*, 31 Annual Report American Bar Association 911 (1907)

PROSSER W., *Privacy*, 48 California Law Review 383 (1960)

PYUN G., *The 2008 Pro-Ip Act: The Inadequacy Of The Property Paradigm In Criminal Intellectual Property Law And Its Effect On Prosecutorial Boundaries*, 19 DePaul J. Art Tech. & Intell. Prop. L. 355 (2009)

RASMUSSEN M.K., *Lobbying the European Parliament: A necessary evil*, Centre for European Policy Studies, May 2011, at www.ceps.eu/ceps/download/5533

RAUCCI M., *Congress wants to give the RIAA control of your IPod: how the INDUCE Act chills innovation and abrogates* Sony, 4 John Marshall Rev. Intellectual Property Law 534 (2005)

RAYNOLDS K., *One Verizon, Two Verizon, Three Verizon, More? – A Comment: RIAA v. Verizon and How The DMCA Subpoena Power Became Powerless*, 23 Cardozo Arts & Ent. L.J. 343 (2005)

REGAN P., *Legislating Privacy*, Chapel Hill (NC), 1995

REINBOTHE J., VON LEWINSKI S., *The WIPO Treaties 1996: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty: commentary and legal analysis*, London, 2002

RESCIGNO P., *Personalità (diritti della)*, in *Enc. giur. Treccani*, XXIII, Roma, 1990

RESTA G., *Diritti della personalità: problemi e prospettive*, in *Dir. inf. e informatica*, n. 6/2007, 1043

RESTA G., *Identità personale e identità digitale*, in *Dir. inf. e informatica*, n. 3/2007, 511

RESTA G., *Il diritto alla protezione dei dati personali*, in CARDARELLI F., SICA S., ZENO-ZENCOVICH V. (eds.), *Il codice dei dati personali: temi e problemi*, Milano, 2004, 11

REYNOLDS D., *The RIAA Litigation War on File Sharing and Alternatives More Compatible With Public Morality*, 9 Minn. J.L. Sci. & Tech. 977 (2008)

RICCI S., VACIAGO G., *Sistemi* peer to peer*: rilevanza penale delle condotte in violazione dei diritti d'autore e diritti connessi*, in *Dir. Internet*, n. 3/2008, 278

RICCIO G.M, *Il* peer-to-peer *alla luce della sentenza della Corte Suprema sul caso Grokster*, *Diritto di Autore e Nuove Tecnologie*, 2005, 149

RICCIO G.M., *La responsabilità civile degli* internet providers, Torino, 2002

RICCIO G.M., *La responsabilità degli* Internet providers *nel d.lgs. n. 70/03*, in *Danno e Resp*., n. 12/2003, 1157

ROBERTS J.M., GREGOR T., *Privacy: A cultural view*, in PENNOCK J.R., CHAPMAN J.W. (eds.), *Privacy*, New York, 1971, 199

RODOTÀ S., *Diritto, scienza, tecnologia: modelli e scelte di regolamentazione*, in *Riv. critica dir. privato*, n. 3/2004, 357

RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Bologna, 1973

RODOTÀ S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. critica dir. privato*, n. 4/97, 583

RODOTÀ S., *Repertorio di fine secolo*, Roma-Bari, 1999

RODOTÀ S., *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla* privacy, in *Europa e Dir. Privato*, n. 1/2004, 1

ROSENBERG G., *The Hollow Hope: Can Courts Bring about SocialChange?*, Chicago, 1991

ROTENBERG M., *Fair Information Practises and The Architecture of Privacy (What Larry Doesn't Get)*, 2001 Stan. Tech. Law Rev. 1, at http://stlr.stanford.edu/2001/02/fair-information-practices-and-the-architecture-of-privacy/.

RUSHTON M.K.J., JONES V.H.L., *The Tortoise and The Hare: Canadian Legislative Copyright Reforms Race Against Copyright Infringement Over Kazaa And Other New Generation Peer-To-Peer Networks*, 32 AIPLA Q. J. 197 (2004)

RYAN T.J., *Infringement.com:* RIAA v. Napster *and the Was Against Online Music Piracy*, 44 Ariz. L. Rev. 495 (2002)

SARTOR G., *Legal Reasoning: A Cognitive Approach to the Law*, in PATTARO E. (ed.), *A Treatise of Legal Philosophy and General Jurisprudence*, Vol. 5, Dordrecht, 2008

SCACCIA G., *Il bilanciamento degli interessi in materia di proprietà intellettuale*, in UBERTAZZI L.C. (ed.), *AIDA - Annali italiani del diritto d'autore, della cultura e dello spettacolo*, vol. XIV, Milano, 2005, 198

SCASSA T., *Recalibrating Copyright Law? A Comment on the Supreme Court of Canada's Decision in* CCH Canadian Ltd. v. Law Society of Upper Canada, 3 CJLT 89 (2004)

SCHULTZ J., *The False Origins of the Induce Act*, 32 Northern Kentucky Law Review 527 (2005)

SCHULTZ M.F., *Copynorms: Copyright and Social Norms*, in YU P.K. (ed.), *Intellectual Property and Information Wealth*, Westport, 2006, 201

SCHULTZ M.F., *Reconciling Social Norms and Copyright Law: Strategies for Persuading People to Pay for Recorded Music*, 17 Journal Intell. Prop. Law 59 (2009)

SCORZA G., *Il conflitto tra copyright e privacy nelle reti Peer to Peer: il caso Peppermint – Profili di diritto interno*, in *Dir. Internet*, n. 5/2007, 465

SELTZER L.E., *Exemptions and fair use in copyright : the exclusive rights tensions in the 1976 Copyright act*, Cambridge, 1978

SHAYESTEH S.A., *High-Speed Chase On The Information Superhighway: The Evolution Of Criminal Liability For Internet Piracy*, 33 Loyola Of Los Angeles Law Review 183 (1999)

SHERWIN E., *Features of Judicial Reasoning*, in KLEIN D., MITCHELL G. (eds.), *The Psychology of Judicial Decision Making*, New York, 2010, 121

SICA S., *Sicurezza e riservatezza nelle telecomunicazioni: il d.lgs. n. 171/98 nel "sistema" della protezione dei dati personali*, in *Dir. informazione e informatica*, n. 4-5/1998, 775

SINGER M.A., *The Failure of the PRO-IP Act in a Consumer-Empowered Era of Information Production*, 43 Suffolk U.Law Review 185 (2009)

SIROTTI GAUDENZI A., *Il nuovo diritto d'autore La tutela della proprietà intellettuale nella società dell'informazione*, Sant'Arcangelo di Romagna, 2008

SIROTTI GAUDENZI A., *Violazione della proprietà intellettuale: non è ammesso il provvedimento di* discovery *in caso di* peer to peer, in *Giur. it*., n. 7/2008, 1742

SMITH EKSTRAND V., *Unmasking Jane and John Doe: Online Anonymity and the First Amendment*, 8 Comm. L. & Pol'y 405 (2003)

SOLOVE D.J., *A Taxonomy of Privacy*, 154 U. Pennsylvania Law Review 477 (2006)

SOLOVE D.J., ROTENBERG M., *Information privacy law*, New York, 2003

SOLOVE D.J., SCHWARTZ P.M., *Information privacy law*, New York, 2009

SOLOVE D.J., SCHWARTZ P.M., *Privacy, Information, and Technology*, New York, 2009

SOLUM L.B., *Procedural Justice*, 78 S. Cal. L. Rev. 181 (2004)

SOMA J.T., RYNERSON S.D., *Privacy Law, Privacy Law in a Nutshell*, St Paul, 2008

SOOKMAN B.B., *Case Comment: Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Service Providers*, 3 Canadian Journal of Law & Technology 149 (2004)

SOOKMAN B.B., *Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions*, Toronto, 2005

SOVERN J., *Opting in, opting out, or no options at all: the fight for control of personal information*, 74 Washington Law Review 1033 (1999)

SPEDICATO G., *Postille in tema di responsabilità extracontrattuale del* provider *alla luce del recente Decreto Legislativo n. 70/2003*, in *Ciberspazio e diritto*, n. 3/2003, 155

SPIRO H.J., *Privacy in comparative perspective*, in PENNOCK J.R., CHAPMAN J.W. (eds.), *Privacy*, New York, 1971, 121

STATEN M.E., CATE F.H., *The impact of opt-in privacy rules on retail credit markets: a case study of MBNA*, 52 Duke L.J. 745 (2003)

STEINMETZ R., WEHRLE K., *Peer-to-peer systems and applications*, Berlin - New York, 2005

SULLIVAN K.M., GUNTHER G., *Constitutional Law*, New York, 2007

TABATABAI F., *A Tale of Two Countries: Canada's Response to Peer-to-Peer Crisis and What It Means for the United States*, 73 Fordham Law Review 2321 (2005)

TAYLOR L., CONNELLY C., *FBI shuts down Megaupload.com, Anonymous shut down FBI*, news.com.au, January 20, 2012, at http://www.news.com.au/technology/fbi-shuts-down-megauploadcom-charges-seven-with-online-piracy/story-e6frfro0-1226249114650

TERRACINA D., *Lucro e profitto nella giurisprudenza della Corte di Cassazione in materia di violazione del diritto d'autore e dei diritti connessi*, in *Dir. Internet*, n. 3/2007, 259

TOLONE A., *La disciplina degli obblighi di conservazione dei dati telematici da parte dei* providers, in *Riv. informazione e informatica*, n. 6/2008, 856

TRIBE L.H., *American Constitutional Law*, New York, 1988

TROTTA A., *Il traffico telefonico fra la tutela del diritto d'autore e quella della* privacy, in *Dir. Industriale*, n. 1/2008, 76

TWU J.C., *Inducing Infringement of Copyrights Act of 2004: FindLaw Interview with John Hughes and Jennifer M. Rich of Townsend and Townsend and Crew LLP*, at http://library.findlaw.com/2004/Sep/27/133584.html

TYLER T.R., *Compliance with intellectual property laws: a psychological perspective*, 29 N.Y.U. Journal of International Law and Policy 219 (1997)

U.S. COPYRIGHT OFFICE, *Summary of The Digital Millennium Copyright Act of 1998*, at www.copyright.gov/legislation/dmca.pdf

VAVER D., *Copyright Law*, Toronto, 2000

VIJAYAN J.**,** *Protests against SOPA, PIPA go viral. Google, Wikipedia, Reddit, BoingBoing plan unprecedented Internet 'strike' Wednesday*, Computerworld.com, January 17, 2012, available at http://www.computerworld.com/s/article/9223496/Protests_against_SOPA_PIPA_go_viral

WALKER J., SOSSIN L., *Civil Litigation*, Toronto, 2010

WARREN S.D., BRANDEIS L.D., *The Right to Privacy*, 4 Harvard Law Review 193 (1890)

WEBBER J., *Culture, legal culture and legal reasoning: a comment on Nelken*, 29 Australian Journal of Legal Philosophy 27 (2004)

WESTIN A.F., *Privacy and Freedom*, New York, 1967

WHITMAN J.Q., *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 Yale Law Journal 1153 (2004)

WIGMORE J.H., *Evidence in Trials at Common Law*, Boston, 1961

WILDPANER C., *The U.S. Digital Millennium Copyright Act. A Challenge for Fair Use in the Digital Age*, Vienna, 2004

WILKINS R.G., *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 Vand. L. Rev. 1077 (1987)

WILKINSON M.A., *Battleground between new and old orders: control conflicts between copyright and personal data protection*, in GENDREAU Y. (ed.), *Emerging Intellectual Property Paradigm: Perspectives from Canada*, Cheltenham, 2008, 227

WINGROVE T., KORPAS A.L., WEISZ V., *Why were millions of people not obeying the law? Motivational influences on non-compliance with the law in the case of music piracy*, 17 Psychology, Crime & Law 261 (2011)

WRIGHTSMAN L.S., *Judicial Decision Making: Is Psychology Relevant?*, New York, 1999

YIU M., *A New Prescription for Disclosure: Reformulating the Rule for* Norwich *Order*, 65 U. Toronto Fac. L. Rev. 41 (2007)

YU P.K., *Six Secret (and Now Open) Fears of ACTA*, 64 S.M.U. L. Rev. 975 (2011)

ZENO-ZENCOVICH V., *Personalità (diritti della)*, in *Digesto disc. priv.*, *sez. civile*, XIII, Torino, 1995, 430

ZILKHA G., *The RIAA's Troubling Solution to File-Sharing*, 20 Fordham Intell. Prop. Media & Ent. L.J. 667 (2010)

ZUCKERMAN A., *Zuckerman on Civil Procedure*, London, 2006

ZWEIGERT K., KÖTZ H., *An introduction to comparative law*, Oxford, 1998