Online Piracy and Copyright Protection Through Internet (A Critical Review For The Intellectual Rights And Obligations Balance)

Edmon Makarim [1]

Internet as a new communication medium, is the result the information and communication technology convergence, which came in the form of an electronic system. In the intellectual property rights perspective especially in copyright context, an intellectual creation is protected as one's property (a bundle of rights) that includes moral rights and economic rights. IPR protection paradigm actually dominated by private communication paradigm, so any communication of the intellectual work is the author's rights. Meanwhile, paradigm in the Internet is a mass communication, so the delivery and retrieval of any information communicated on the Internet is considered as the rights of every human being. These differences seemed lead to the ineffectiveness of any attempt to restrict copying or access to the use of a digital work.

Keywords: *online piracy, copyright protection, internet*

I. Introduction

Nowadays, communication system has evolved from centralize telecommunications circuit switching based model to a distributed global communication medium that on packet-switching- based using Internet protocol (TCP / IP). This kind of communication system offers speed but on the other side has communicating security weakness because it is built upon the principle of connection[2]. On the conventional telecommunications, it has obvious transmitter and receiver through dedicated connection. On the Internet, communication focuses on the certainty of information delivery which sent randomly in packets and then reassembled at the

1 Senior Lecturer and Researcher of Telematics Law, Faculty of Law University of Indonesia.

2 Schweitzer, Douglas., Internet Security Made Easy., New York: AMACOM, 2002.

destination point through all available channels. Technically information distribution through the internet is intended to spread information easily but unpreventable. It seems that Internet characteristics built as mass communication not as private communications.

Internet as a new communication medium, is the result the information and communication technology convergence, which came in the form of an electronic system. This convergence resulted from the merging of the two communication paradigms, the confidential communications paradigm between the parties, and the public or open mass communications paradigm. In one particular context, communication on the Internet can not be said to be an announcement, but in the other hand, it can be considered as an act of the announcement. But certainly, all the information in the digital environment are communicated through duplication or copying. There is temporary information duplication that only intended to read-only, and there is a permanent duplication as intended to store information itself.

Meanwhile, various information communicated via the Internet is increasingly diverse due to the development of digital technologies. Started with an analog system in the form of voice and text, and now communicated information includes all possible forms, such as images, data, documents, videos, and so forth. It also resulted that Internet known as multimedia facilities. Subsequently, the Law of the Internet will include the convergence of the legal paradigm of telecommunications, media and information (telecommunications), with three-layer focused regulation approach, namely: (i) regulation of resources, (ii) regulation of infrastucture and access, and (iii) regulation on the application and content.

Many benefits can be provided by the Internet, but there are those who abuse it for self-benefit and might against the law. For example, the distribution of illegal content, which might include the distribution of digital intellectual creations (digital works)[3] without permission or without right or without legitimate interest.

In the intellectual property rights perspective especially in copyright context, an intellectual creation is protected as one's property (a bundle of rights) that includes moral rights and economic rights. To protect the moral rights and economic rights, formally, any duplication or copy by other par-

3 In general, digital works are any intellectual creations or creations that can be represented in digital form or in other words can be represented by a binary code (0 or 1), including: photos, songs, music, electronic books, databases, computer programs, etc. . Meanwhile, based on the nature of the data is divided into (i) fixed data (eg songs, music, databases and other similar things), and (ii) the dynamic data which is a series of instructions for the operation of a particular function (eg computer program).

ties should be done with the permission of the creator, if not then it is a violation (infringements)[4]. Therefore, the creator has the right to control every form of duplication and / or announcement to the public. But on the other hand, Internet is a global communications medium that works on the basis of the certainty of technical operation in which each information delivered and accepted between the parties. Communication providers involved did not check or control the communicated content, so the responsibility for the communicated content is on the users.

IPR protection paradigm actually dominated by private communication paradigm, so any communication of the intellectual work is the author's rights. Meanwhile, paradigm in the Internet is a mass communication, so the delivery and retrieval of any information communicated on the Internet is considered as the rights of every human being. These differences seemed lead to the ineffectiveness of any attempt to restrict copying or access to the use of a digital work.

II. Application of Copyright on the Internet

As described before, copyright protection on Internet focussing to any attempt to restrict access and usage of the creation. Things that considered as a violation is all activities that involve copying or make the work available to public without permission (eg, linking, framing, sharing/P2P, etc.).

To prevent these kind of violations, specific technologies (eg encryption) is used so everybody can not easily make a copy (copy control measures), access (access control measures), or change any information attached to a creation (rights management information). Information Technology provides several ways to do locking, such as using CSS, DeCSS, dongles, etc. As a consequence, it is necessary to have legal protection mechanisms by providing a legal obligation for everyone to appreciate the security system, where the breach of it will make the injured party be entitled to sue redress.

Ironically from time to time, the efforts to defend the rights of creations was always getting resistance from the other parties who are keen so an intellectual creations can freely accessible to public regardless the restrictions of its exclusivity (jail-break). Some of it considered this as a

4 In the United States there are several categories of violations, namely: (i) Direct Infringement; (ii) Contributory Infringement; (iii) Vicarious Infringment; dan (iv) Inducing Infringement.

matter of fair use, because it is done on the basis of a legitimate motivation (eg. reverse engineering to create an interface in the framework of inter-operability with other computer systems programs, encryption research for repair, improvement or further development), but some other do with the motivation to take advantage.

Besides the technical protection efforts, creators can also perform administrative efforts for the sake of proving when necessary, by registering his creation on copyright registration office. Actually, this mechanism does not prove the originality of a copyrighted work, but used only for initial evidence that the person concerned is the actual creators, if necessary.

III. Critical Analysis

It is very interesting if we look deeper to the philosophical and sociological conditions of how the Internet is becoming popular. At the beginning, the Internet project was initiated by the Defense Advance Research Project Agency switched network (ARPANET), which then combined with an academic network of the National Science Foundation Net (NSF-NET), and then developed to the public not only for social communication purposes but also for the commercial purpose. At that time there has been a clash of paradigms and interests of the parties who have an interest in the Internet[5]. Chris Reed said that it is a shift of the reduction in private property absolutism that prevents other people to access and then become the global property where many people have access to information resources, in other words 'property' became 'propriety'[6].

As a medium dominated by the paradigm of freedom of expression, freedom of communication, and freedom to access information, Internet became a means to access knowledge for its users. The desire to share and enhance each other are the motivation that should be appreciated by all those who involve into this network universe. Honesty and openness of expression without having a cover-up became the paradigm which typically were found[7]. Not only within the scope of information disclosure inorder to

5 Andrew D. Murray, The Regulation of Cyberspace: Control in the Online Environment., New York: A Glasshouse book., 2007., p. .60-73.

6 Chris Reed., Internet Law: Text and Materials (2nd edition). Cambridge: University Press, 2004. p. 88.

7 Lawrence Lessig, Code and Other Laws of Cyberspace. New York: Basic Books, 1999.

implement good governance in all aspects but also the clarity of information on a product before a transaction of goods and/or services traded.

The same thing applied to the clarity of information of digital products (eg. computer program) within the Internet that offered to all internet users as consumers across the country. Most users will ask for honesty and openness of reliability even the openness of expression in the programming itself that represented an instruction as a form of expression that conveyed the idea that became apparent as they are, so trust on the reliability of the system offered including the risks. So it would not be a transaction barrier because performed with honest and fair by all parties[8]. Apparently it is one of the reasons why the 'open source' movement would be the answer for society to be able to access the substance of an intellectual work as a whole, making it quite popular among academic activists in this field.

Ironically, for the pretext of greater interest, it seems that the perspective of sentencing in copyright only represent the interests of industrialists in which a society is threatened as the external potential abuser. In other words, the crime formulation is often placed only on the external scope of the developers which are the competitors or the users. There only a little discussion of the criminal perspective that put the obligations of the intellectual/creator to the public or to the right holder, if it turns out that the product they made affects a great loss to the public or the users as consumers. However, if truly there is a balance of interests, so clarity of rights protection must be follow by clarity of obligations execution.

In the context of the Internet, an electronic information in the form of binary code (0 or 1) in fact not only can be seen visually as shown information but it can also be potentially compromised by an invisible code in it. It does not only occur due to external parties but also occurs from the internal side. Similarly, a set of instructions that works as a computer program, may be had a destructive instruction that will work later on. One should aware that the real potential criminals not only dominated by the user perspective but also from the developer or the vendor itself may have possibility to misuse their right to lock the competition through innovation (IP abuse) with Another competitor, which in turn will adversely affect the public as consumers.

8 Prins, J.E.J., & Ribbers, P.M.A., et. al., Trust in Electronic Commerce: The role of Trust from Legal, an Organizational and Technical Point of View. Netherlands: Kluwer, 2002. p. 1-41.

V. IPRs Abuse and Criminalization (IP abuse vs. Criminalization)

In accordance with article 7[9] and article 8[10] TRIPS, IPR system not only gave birth to the protection of private rights but also the protection of the public interest to encourage technological development, transfer of technology, and prevent the abuse of IPR that may hinder fair competition or impede action the transfer of technology.

Under Article 40 paragraph (1)[11] and (2) TRIPS, there is possibility that the existence of the licensing can be misused to impede fair competition and it will make inhibition tor development of the technology itself and its spreading to the public. Unfortunately the formula was not further regulated or at least accompanied by a formulation of how obligation or liability of the owner of the intellectual should be executed and what the threat if it is not executed.

While on the other hand, article 61[12] of the TRIP's mandates that member states shall make provision for punishment (imprisonment and / or

---

9 Article 7 Objectives: The protection and enforcement of IPR's should contribute to the promotion of technological innovation and to the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations.

10 Article 8: (1) Members may, in formulating or amending their laws and regulations, adopt measures necessary to protect public health and nutrition, and to promote the public interest in sectors of vital importance to their socio-economic and technological development, provided that such measures are consistent with the provision of this agreement. (2) appropriate measures, provided that they are consistent with the provisions of this agreement, may be needed to prevent the abuse of IPR's by right holders or the resort to practices which unreasonably restrain trade or adversely affect the international transfer of technology.

11 Article 40: section (1) Members agree that some licensing practices or conditions pertaining to intellectual property rights which restrain competition may have adverse effects on trade and may impede the transfer and dissemination of technology. Section (2): Nothing in this Agreement shall prevent Members from specifying in their legislation licensing practices or conditions that may in particular cases constitute an abuse of intellectual property rights having an adverse effect on competition in the relevant market. As provided above, a Member may adopt, consistently with the other provisions of this Agreement, appropriate measures to prevent or control such practices, which may include for example exclusive grantback conditions, conditions preventing challenges to validity and coercive package licensing, in the light of the relevant laws and regulations of that Member.

12 Article 61: Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence.

fines) against commercial copyright piracy done intentionally (committed willfully and on a commercial scale). It is understandable that the provision is addressed to the parties that take advantage as a seller, similar to the production of goods with counterfeit brand (trademark counterfeiting). Based on the research, the mandate to criminalize this kind of action not found explicitly in the TRIP's, but it only regulated who conduct discontinuation and seizure or remove the item so that it can no longer be used.

This assumption is the consequence Article 60[13] TRIPS which states that member states may exclude the trading inhibition at the country border (cross country) if it is not intended for commercial purpose in personal luggage in small amounts (travelers' personal luggage) or delivered as small consignment.

Under these provisions, developing countries should take notes why developed countries at that time did not balance the interests between the rights and obligations as mandated in the TRIPS article 7. If there is an obligation to criminalize the external parties to intellectual work, there should be an obligation to criminalize those who abuse the IPR. IPR abuse will had a strategic impact on public order or public interest, so it should have to be regulate the confinement and / or penalties against it. But unfortunately there is no such provision, but only provides a means of settlement and consultation between the parties only[14].

Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.

13 Article 60 De Minimis Imports: Members may exclude from the application of the above provisions small quantities of goods of a non-commercial nature contained in travellers' personal luggage or sent in small consignments

14 Article 40 section (3): Each Memnber shall enter, upon request, into consultations with any other Member which has cause to believe that an intellectual property right owner that is a national or domiciliary of the Member to which the request for consultations has been addressed is undertaking practices in violation of the requesting Member's laws and regulations on the subject matter of this Section, and which wishes to secure compliance with such legislation, without prejudice to any action under the law and to the full freedom of an ultimate decision of either Member. The Member addressed shall accord full and sympathetic consideration to, and shall afford adequate opportunity for, consultations with the requesting Member, and shall cooperate through supply of publicly available non-confidential information of relevance to the matter in question and of other information available to the Member, subject to domestic law and to the conclusion of mutually satisfactory agreements concerning the safeguarding of its confidentiality by the requesting Member. Section (4) A Member whose nationals or domiciliaries are subject to proceedings in another Member concerning alleged violation of that other Member's laws and regulations on the subject matter of this Section shall, upon request, be granted an opportunity for consultations by the other Member under the same conditions as those foreseen in paragraph 3.

The next progression is the existence of the WIPO Copyright Treaty (WCT) and the WIPO Phonograms Treaty and Performer ("WPPT") in 1996. Both instruments states the need to maintain a balance between the rights of the creators (authors) and related rights (rights of performers and producers of phonograms) with a larger public interest, especially for educational purposes, research, and access the information as presented in the Berne Convention.

WCT confirmed that Computer Programs in any form and Compilations of Data (database) is an object that is protected as the work of science in the article 2 in the Berne Convention. WCT treaty clearly explain the existence of Distribution Rights (Right of Distribution) which includes[15] (i) the exclusive right to grant permission to the original work or the copy available to the public, either through sales or through other ownership rights transfer, (ii)Right of Rental, if it is an essential object, and (iii) Right of Communication to the Public that includes electronic transmission. Furthermore, it also state the obligation that every person have to protect technological protection means (Obligation Concerning Technological Measures[16]) used by the creators or copyright holders to restrict access to his creation, and the obligation to respect the integrity of information of the creation (Obligation Concerning Rights Management Information[17]) so any person can not change the information related to ownership that inherent in creation.

---

15 Article 6 WCT: Authors of literary and artistic works shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their works through sale or other transfer of ownership

16 Article 11 WCT, Obligations concerning Technological Measures: Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.

17 Article 12, Obligations concerning Rights Management Information: (1) Contracting Parties shall provide adequate and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention: (i) to remove or alter any electronic rights management information without authority;(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority. (2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

The question is whether those obligations have demonstrated the balance between intellectual property rights and obligations, because the perspective is not an obligation of the creator but the presence of an external party's obligation to the Creator against the Creation. Then, how about the certainty of access to information and educational interests and research to study these creation, do they could do reverse engineering. Surely it would be a clash between the obligation to maintain technology control with the right to reverse engineering that allowed by about Trade Secrets Act.

Associated with crime aspects, copyright infringement back on the discussion at the Convention on Cybercrime in 2001 and including the strategic discussion on asset protection that are included in the discussion of Cybersecurity.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article

It is interesting that in the paradigm of the European Convention, a member state may not make the criminal formulation if there are other provisions that could effectively restore the rights of the aggrieved party. This development also should be the concern of other countries, that the demand of the criminal formulation does not always have to be applied implicitly as a means of recovery of loss or as a means of preventing infringement.

As a comparison, US has a policy concerning the limitation of fair use principle, based on Article 17 USC Section 107 (2000), that consider four factors:

a. the Purpose and character of the use, including whether such use is of a commercial nature or for non profit educational use;
b. the Nature of the copyrighted work;
c. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
d. the effect of the use upon the potential market for the work or value of the copyrighted work.

After that, there is criminal formulation found in the Section 1201 US Digital Millenium Act (DMCA) concerning circumvention of copyright protection system, that work differently far beyond WCT. DMCA prohibit anyone who intentionally break the protected creation that distributed closely for commercial purpose. This is causing critics from experts because this has overstep the commitment mandated by WCT.

- No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.
- No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that - (A) is primarily designed or produced for

the purpose of circumventing a technological measure that effectively controls access to a work protected under this title; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

Similar to the US, Indonesia also had criminal formulation of copyright infringement that is expected to prevent violation. Unfortunately, the criminal formulation is inappropriate because it is not as mandated by the TRIPs in the application of "committed wilfully and on a commercial scale" where it is not intended to end users.

For example, if someone has purchased a license for one copy and then reproduce it on a his own device, then this can not be said as an infringement that based on the number of licenses, copy, and the usage quantity because it is based on his legitimate interest that enabling him to access the creation at his various device (internal puporse only). It should be protected by the First Sale Doctrine. But it becomes different when it expands its use by exchange it to another party or distribute it and resulting loss to the copyright holders.

Moreover, Article 14-28 Indonesia Copyright Act has also been too narrowly limit the scope of 'fair use' that only allowed for research activities, educational and other non-commercial activities. Compared to the US, it should have opened the possibility to test the four factors mentioned above in each case. By doctrine, using without permission can not be regarded as an infringement as long as not violating the principle of moral right and the right of reasonable economic interests. Too limited determination of fair use will cause injustice behind the day.

Before the Internet widely used for commercial purposes, the perspective on the Internet is dominated by the freedom of expression and public access to science development. In this context, any digital work is considered as a common interest, so the examination and substance revealing of an intellectual work (hacking) is not considered as a crime because it is done to improve the work itself and is a way of learning to improve society. This also applies to any act of copying or multiplication, because in the

Indonesian Law	Explanatory
Article 72 of Copyright Law	
(1) Any person who deliberately and without rights commits acts as referred to in Article 2 paragraph (1) or Article 49 paragraph (1) and paragraph (2) shall be punished with imprisonment of at least 1 (one) month and / or a fine at least Rp 1,000,000.00 (one million rupiah), or a maximum imprisonment of 7 (seven) years and / or a maximum fine of Rp 5,000,000,000.00 (five billion rupiah).	Paragraph (3)
(2) Any person who deliberately broadcast, display, distribute, or sell to the public a work or goods resulting from an infringement of copyright or related rights as referred to in paragraph (1) shall be punished with imprisonment of at most 5 (five) years and / or a fine Rp 500,000,000.00 (five hundred million rupiahs).	
(3) Whoever intentionally and without right to reproduce (duplicate) for commercial use of a computer program shall be punished with imprisonment of 5 (five) years and / or a maximum fine of Rp 500,000,000.00 (five hundred million rupiahs).	What is meant by extending the use of the duplicate, or copy the computer program in source code (source code) or application program.
(4) Whoever intentionally violates Article 17 shall be punished with imprisonment of 5 (five) years and / or a maximum fine of Rp 1,000,000,000.00 (one billion rupiahs).	
(5) Whoever intentionally violates Article 19, Article 20, or Article 49 paragraph (3) shall be punished with imprisonment of 2 (two) years and / or a maximum fine of Rp 150,000,000.00 (one hundred and fifty million rupiah) .	The meaning of the source code is an archive (file) program that contains statements (statements) programming, code instructions / commands, functions, procedures and objects created by a programmer (the programmer).

(6) Any person who deliberately and without rights violates Article 24 (moral right), or Article 55 shall be punished with imprisonment of 2 (two) years and / or a maximum fine of Rp 150,000,000.00 (one hundred and fifty million rupiah).	
(7) Any person who deliberately and without rights violates Article 25 (rights management information) shall be punished with imprisonment of 2 (two) years and / or a maximum fine of Rp 150,000,000.00 (one hundred and fifty million rupiah).	For example: A computer program with the right to buy licenses for use on a single computer unit, or B entered into a licensing agreement for use of a computer program application on 10 (ten) computers. If A or B duplicate or copy a computer program application on top for more than a predetermined or agreed upon, the action was a violation, except for the archives.
(8) Any person who deliberately and without rights violates Article 27 (technological measures) shall be punished with imprisonment of 2 (two) years and / or a maximum fine of Rp 150,000,000.00 (one hundred and fifty million rupiah).	
Article 32 UU ITE (Data Interference)	Elucidation of Article 32: Sufficiently clear
(1) Any Person who knowingly and without authority or unlawfully in any manner whatsoever alters, adds, reduces, transmits, tampers with, deletes, moves, hides Electronic Information and/or Electronic Records of other Persons or of the public.	
(2) Any Person who knowingly and without authority or unlawfully in any manner whatsoever, moves or transfers Electronic Information and/or Electronic Records to Electronic Systems of unauthorized Persons.	

(3) Acts as intended by section (1) shall be acts that result in any confidential Electronic Information and/or Electronic Record being compromised such that the data becomes accessible to the public in its entirety in an improper manner.	
Article 33 UU-ITE (System Interference)	Elucidation of Article 33: Sufficiently clear
Any Person who knowingly and without authority or unlawfully commits any act resulting in faults on Electronic Systems and/ or resulting in Electronic Systems working improperly.	
Article 34 UU-ITE (Misuse of Devices)	Elucidation of Article 34 Section (1):
(1) Any Person who knowingly and without authority or unlawfully produces, sells, causes to be used, imports, distributes, provides, or owns:	Sufficiently clear
a. Computer hardware or software that is designed or specifically developed to facilitate acts as intended by Article 27 through Article 33;	
b. Computer passwords, Access Codes, or the like to make Electronic Systems accessible with the intent to facilitate acts as intended by Article 27 through Article 33;	Elucidation of Article 34 Section (2):
(2) Acts as intended by section (1) are not criminal acts if aimed at carrying out research activities, testing of Electronic Systems, protection of Electronic Systems themselves in a legal and lawful manner.	"Research activities" shall be research that is
	conducted by authorized research institutions.

digital environment 'reading' (viewing) means that the material is loaded to computer memory (loading), which is also created a copy.

Similarly, sending a copy to another party to be studied (sharing) is considered as a distribution to improve the quality of science itself, not as a distribution in commercial selling. Critics on the system reliability is a very common thing and it is very necessary to improve the opertion quality of the network.

It is a different issue when the Internet has become the place for business commercialization. Industrialization interests demand that each person should not exploit any vulnerability on another party, because there is no perfect work that free from mistakes, meanwhile it cost them investment in improving the work. The computer program never be free from the potential errors in programming (bugs), therefore program developer licensed it by saying as they are ('as is').

If errors are known and the impact affect seriously on losses, it will certainly open the possibility to ask for responsibility based on defective products. For the sake of the industry growth, developed countries seem to keep it unreavealed than being known by the public. Putting trade secrets under a reasonable interest to the value of comparative or competitive advantage of a creation is a good reason to get legal protection. The question here, where the equilibrium that mandated by Article 7 TRIPS is, although commonlly the work is not traded so the rights remain on the creator. Then what happens if our products damaging items/systems of others who already using it and install it on his digital space?

Generally, the standard license agreement offered to the public has waived the responsibility by claiming the absence of a standard warranty of trade worthy (merchantability) and there is no guarantee of appropriateness to the benefit needed by the user (fitness for particular purposes). It only can give a guarantee of technical support according to ability and duration of their R&D investment in product development, although royalties have been paid in advance without formulating a specific period of time. That only if the user violates the manufacturer's standard contract, so creator should not be responsible anymore.

On later progress, it seems that the protection of IPRs has negating opportunities for the science and technology to develop, by cover up something that should open, so there arose resistance movement against greediness in taking advantage of an intellectual creation. It represented by shifting private rights idea which seems so absolute (all rights reserved) to

respecting the public interest (public domain), such as by use of the 'copyleft', sharing, or free use. This two-sides of interest has confusing the public because it seems there are two different legal regimes on IPRs. Indeed both the 'copyright' and 'copyleft' are constructed on legal system, especially the enforceability of copyright law to balancing the rights of creators with the right of the public.

This confusion remains unanswered until the rise of the central axis movement which moderately bring the copyright to its basic nature properly. This movement carried by Lawrence Lessig with his 'Creative Commons License' movement (CCL). The movement is built based on 'Some Rights Reserved' term in which the creators are not retained all rights but only part of it. CCL provides an alternative between society and creator, so they could get away from industrialists domination as the holder of the Copyright, particularly in exploiting the economic value of the creations. Through the CCL, the Creator can choose to distribute his work to the public directly as they wish with several alternative licensing models provided. In fact, the creators also need to share contents and get response or comment of his creation from the public, but they can still restrict any commercial use of it, indeed the relevant interests should not be eliminated.

The 'not take the direct economic benefits' argument are commonly expressed by every person who believes that what they do is based on 'fair use'. Especially if they get it from public domain and used only for its own purpose (internal purpose only). But on the other hand, the reason could be misused if it turns out that the distribution done intentionally and con-

(c) all rights reserved	(cc) some-rights reserved	(pd) public domain all rights are retained by the creator or copyright holder
some right retained and others granted to the public	all rights granted to the public	

sciously to cut off the economic value of the parties who have legitimate interest.

The classic example of such violations on the Internet which involve illegal song exchanged either directly or by file-sharing systems between users, are very difficult to prevent. In fact, not all file-sharing system with Peer-to-Peer system (P2P) is against the law, so the criminalization of such systems is must be done carefully.

Previously, such violations can be easily proven because P2P is still centralized, but when it decentralize, the abuse is relatively difficult to prove. Same thing applied to the abuse on Content Protection destruction[18]. Along with the use of encryption technology development, the development on decryption software tools is rising. Meanwhile, the infringement against a change in the creation information management on the Internet seems rarely happens. It indicates that the distribution on the Internet, generally not intended to possess, move, acknowledges the copyright of the creators, but just take the economic advantage of the creations.

As described before, it seems that any efforts to limit access and prevent the spread of illegal content would be very difficult, especially if it does not involve the intermediary parties on the Internet itself (intermediary services). It will be more effective if prevention and mitigation involving the itermediary parties, which it could put obligations to provide a reporting or public complaints mechanism legally (notice and take-down policy) if there is a distribution of illegal content on their services.

By this mechanism, they can inhibit or at least minimize the access to it or even make suspension or removal if such creations found on their services. To perform the mechanism, they need legal protection against the potential countercharges of the illegal content publisher. Therefore, it is necessary to provide legal provisions concerning limitation of the intermediaries liability which could be incorporated either in the Copyright Act, the Telecommunications Act or the Electronic Commerce Act.

VI. Indonesia Case Studies

Recently, Indonesia law enforcement officers implementing the criminal formulation on the Copyright Act that criminalize those who use the

18 International Telecommunication Union, Understanding Cybercrime: A guide for developing countries, ITU Publication, 2009.

US	EU Directive
§ 512. Limitations on liability relating to material online	Article 12 – "Mere conduit"
(a) Transitory Digital Network Communications	1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if –	(a) does not initiate the transmission;
(1) the transmission of the material was initiated by or at the direction of a person other than theservice provider;	(b) does not select the receiver of the transmission; and
(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;	(c) does not select or modify the information contained in the transmission.
(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;	2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than isreasonably necessary for the transmission, routing, or provision of connections; and	3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.
(5) the material is transmitted through the system or network without modification of its content.	
	Article 13 – "Caching"
(b) System Caching	1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information'sonward transmission to other recipients of the service upon their request, on condition that:
(1) Limitation on liability.– A service provider shall not be liable for monetary relief, or, except asprovided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which –	(a) the provider does not modify the information;
(A) the material is made available online by a person other than the service provider;	(b) the provider complies with conditions on access to the information;
(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and	(c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.	(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 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.
§ 230. Protection for private blocking and screening of offensive material	2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.
(c) Protection for "Good Samaritan" blocking and screening of offensive material	
(1) Treatment of publisher or speaker No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.	Article 14 – Hosting
(2) Civil liability	1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

No provider or user of an interactive computer service shall be held liable on account of –	(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
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent,harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or	(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).	2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
	3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.
	Article 15 – No general obligation to monitor
	1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

	2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities,at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

program without a license or using a computer program exceeds the limits of the license obtained. While on the other hand, it seems that people has trapped to a monopolistic conditions or being controled by device hegemony and leaving them with no choices. Therefore, if this condition was intentionally happens, it should be questioned[19].

According to that, there is inaproppriate implementation in Indonesia system. Thus, allow me to state some cases position i have observed.

1. In Surabaya, an internet cafe sued under the infringement of Copyright on Rental Right on the operating system they used, even though they already have licensed operating system on their computers. In this context, it should be seen clearly what kind of services they provide, whether they rented the OS and the browser or the internet acces services, because actually they provide internet access services and not a OS and office applications rental.
2. In Karawang, there is a company downloaded an antivirus program and use it internally. Previously they had licensed antivirus program but not working effectively, so they look for another antivirus programs on the Internet. Unfortunately, they gained the antivirus program from a site that have no right to distribute it. When they had an inspection on them, the unlisenced antivirus program found on their system, and

19 Normally an act considered as criminal act should be based on two things, namely (i) wrongdoing (actus reus) with bad intentions based on the intent, and (ii) (mens-rea). It seems that the criminal formulation on the Copyright Act actually become counterproductive to the purpose of copyright legal system itself. People who unknowingly contaminated by the popularity of a product and did not find substitute products in an alternative markets tend to be forced to use and had to be convicted because using illegal products.

then they sued under Article 72 paragraph (3) Indonesia Copyright Act.

3. In Surabaya, a Digital printing company (SME's) sued under infringement of copyright because they using some unlicensed softwares that. This case is similar to the internet cafe case above, they considered using the software rented to public. They actually use the software limitedly to reading files. The company owners sued under article 72 paragraph (3) Indonesia Copyright Act.

Compared with the US, if the fair-use test is applied to the three cases mentioned above, we will found some interesting facts.

Measuring Point	Internet Cafe	Antivirus	Digital Printing
1. The purpose and character of the use;	• Computer rental for internet access services	• Internal usage	• Files reading and printing
2. The nature of the copyrighted work;	• Operating System (computer program)	• Antivirus program	• Operating system and CAD Program
3. The amount and substantiality of the portion used;	• Lisenced Operating System for each computer they use/	• Used on internal network computer	• Multiple use on internal computer
4. The effect of the use upon the potential market for the work or value of the copyrighted work.	• Did not affect potential market	• Did not affect potential market	• Did not affect potential market

Specifically on computer programs, law enforcement should be applied fairly by recognizing the characteristics of computer programs[20], the exercise, and nature of the industry first, before applying the criminal procedure to the violators.

But firstly, there is a misinterpret error on Article 72 paragraph (3) explanation between the formulation and the examples presented there. It

20 In accordance with Article 1 Paragraph (8) Law 19/2002 on Copyright, a computer programs are a set of instructions expressed in the form of language, codes, schemes, or any other form, which when combined with media that can be read by computers will enable computers work to perform specialized functions or to achieve specific results, including preparation in designing these instructions. Compare it with the definition in the WCT that states cover all modes and forms.

equalize Source Code with Object Code, at the same time possession of the Source Code and Object Code will have different consequences. Possession of the Object Code does not result in the modification, meanwhile possession of the Source Code actually resulted in any possessor seemed to be the owner because they can modify either the title or the literal programming. So the example given was not congruent with the proper explanation.

A further question rise whether the 'increase the use for commercial purpose' is intended to commercial propagation or to the consequences of commercial use of a computer program.[21]

To answer it, we have to understand that agreement of the computer program is not just as assumed by the Copyright Act makers as only a license, furthermore it include the transfer of copyright (assignment). Based on the industry nature, clearly that the business model exploring economic interests of the Computer Program came in very diverse forms. There are license agreement selling as if it wass a conventional product (eg, non-exclusive and proprietary lisence), and lisence selling as a sale of services only (example: public license). There are two basic types of agreements, namely: (i) the transfer of copyright agreement (assignment of copyright) that transferred the copyright to the users. This applies commonly if computer programs were made based on the request or order, (bespoke software). (ii) license agreement (granting permission to certain rights described in the agreement itself).

The license agreement itself came into several types, namely: (i) exclusive and non-exclusive license, (ii) license agreement with the closed source code and licensing agreements with open source code, (iii) private interests license (eg, End User License Agreement) and public license where the author release some parts of his rights to the public, not only the right to use but also modify and distribute as objects that are placed in Public Domain (iv) a paid license and free license, (v) license for end users only and license for modification and further developed (sub-license).

Considering that the enforceability of the license equivalent to contract, then lisence agreement should referred to the validity of contract (Article 1320 Indonesia Civil Code), particularly on the subjective and ob-

21 It had to keep in mind that in the characteristics of digital environments, all use or reading of a computer program is carried out with a load or copies of a storage media to the media primary access memory (RAM) on a computer, which is also known as "loading" or loading. It is therefore within the scope of Information Technology, each copying an electronically can not be said to necessarily be a violation of copyright. This must be seen in context and characteristics of the license agreement itself first.

jective terms in contract. Therefore, before a license enforced, the agreement validity have to be ensured . If not, then the license could not be put under protection and forced to third parties. If the licensing agreement was contrary to law, then it will become null and void. (Example: contrary to the standard contract determined by the Consumer Protection Law, Law-Human Rights and the Law on Prohibition of Monopolistic Practices and Unfair Business Competition). Therefore, the license violation on using a copyright would be unrelevant if put under criminal law, because the violation based on Law of Contracts and not as violation on criminal act.

Based on previous explanation , clearly there is a formulation missunderstanding of Article 72 paragraph (3), because it assuming on just one type of license only, without making sure the characteristics of the license and the type of industry.

The source code is a string of high-level instruction in a programming language, its existence is like a blueprint of a house construction or a clothes pattern. So if the source code is exposed, everyone will be able to create, modify, or even repair the programs. In other words, possession over the source code causing possessor could act as if they is the owner of the program because they can perform the reengineering of creation. It can be considered as criminal violation (stealing) under the Criminal Code. Meanwhile, the object code is a string of instructions in machine language (low level language) that can only be understood by the machine but can not be understood by humans. In other words, control over an object code causing only limited use without the freedom in using like property rights. So unauthorized usage can not be considerd as criminal violation.

It seems that the Act was intended to every person who is doing the multiplication of pirated goods and resell it as if the genuine products. So he distributed counterfeit products to the public (counterfeiting goods). For instance, selling a pirated program on a piece of CD to the public.

Article 72 would be inaccurate if applied to the possession of Object Code because it is not intended to be the owner and take the commercial rights of the Creator. The economic value by usage is different from commercial rights attached to the industrial value of the computer program itself as a product or service.

If this analysis applied to the three cases above, using a computer program that only for reading and printing files/documents that belong to anyone else, without multiplication/selling the copies to other parties or lease a computer program to others, can not be said as violations to the

commercial rights of the Creator or Copyright Holder (vendor) against the computer program. Apparently, using a copyright as mentioned in the cases did not affect the market share of sales of computer programs itself to the public.

By considering all the criteria of Fair Use and examining the cases, it is clear that the element of 'without right' and 'commercial interests' must be proportionally seen according to each case. In following the mandate to balance the interests between the rights and obligations, criminal prosecution can only be executed if there is already a competitive market condition where people are free to choose and there is no abuse of IPRs.

VII. Conclusion

1. Online piracy should proportionally applied according to the TRIPS and the CoC that only against actions that are intended to take economic interest without right, not as user who only using it by no choice caused by a monopolistic conditions. Therefore, for the criminalization of copyright infringement need to be reviewed and equivalent to the enforcement of competition law in the software industry so that people have much choices in the digital market.
2. Content protection, either directly or indirectly will always get resistance because basically people will always find a way to access closed content. It can be said as fair if only the provisions of Fair Use in Indonesia opened normatively rather than linearly limited.
3. Prevention and control of distribution of illegal content would be effective if it involves the role and responsibilities of intermediary services.

Notes:

Along with the paradigm of a three-tier arrangement in the convergence of telematics (resources, infrastructure, and applications and content) when confronted with this type of layer computer programs (microcode, operating-system, GUI, application), then we see that the competition principle of essential facilities doctrine would apply to the existence of a computer program operating system by the life of content and applications industry. In this context, then any attempt to open an access control to fight

copyright abuse is certainly not feasible for criminalized. Therefore the provisions of criminal prosecution on the matter must be eliminated or at least no longer be applied because it has inhibited greater interest of greater interest in networked electronic communication relations (Inter-Networking) i.e. for interoperability and interconnect with each other.

Bibliography

Bagby, John W. Cyberlaw Handbook for E-commerce. Ohio: Thomson-Souther-Western-West. Bruxelles: Bruylant, 2005.

Cobcroft, Rachel (ed)., Building an Australasian Commons (vol.1)., penerbitan tanpa tahun., http://creativecommons.org.au/casestudiesvol1.

Chissick, Michael dan Allistair Kelman. Electronic Commerce Law and Practice (3rd edition). London: Sweet & Maxwell, 2002.

Landy, Gene K., The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media and IP Law., Burlington: Syngress Publishing, 2008.

Lessig, Lawrence. Code and Other Laws of Cyberspace. New York: Basic Books, 1999.

————————. The Future of Ideas: the Fate of the Commons in a Connected World, New York: Random House, 2001.

————————., Remix: Making Art and Commerce Thrive in the Hybrid Economy, London: Bloomsbury Publishing, 2008

————————., Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity., New York: Penguin Press, 2004.

Murray D, Andrew., The Regulation of Cyberspace: Control in the Online Environment., New York: A Glasshouse Book, 2007.

Prins, J.E.J., & Ribbers, P.M.A., et. al., Trust in Electronic Commerce: The role of Trust from Legal, an Organizational and Technical Point of View. Netherlands: Kluwer, 2002.

Reed, Chris. Internet Law: Text and Materials (2nd edition). Cambridge: University Press, 2004.

Rowland, Diane., Elizabeth Macdonald., Information Technology Law (3rd ed.)., London: Cavendish Publishing, 2005.

Smith,Graham J H., Internet Law and Regulation (3rd ed)., London: Sweet and Maxwell, 2002.

Schweitzer, Douglas., Internet Security Made Easy., New York: AMACOM, 2002.