Sharing Encrypted Data on the Internet – A Grey Area Between Privacy and Intellectual Property Law

Quang Huy Nguyen,[*] Van Nam Tran[**]

ABSTRACT

Online piracy is a current issue, which accompanies file-transferring technology. This problem is magnified by the application of encryption to hide pirated contents. Besides that, encryption is a tool to protect information of Internet users from data breach.

The aim of this paper is to describe the role of encryption in file sharing networks, related to Privacy of Internet users and Intellectual Property rights of content owners. This article proves that both right to Privacy and Intellectual Property rights need to be respected and therefore, the conflict between encryption users and copyright owners is difficult to solve. From this approach, some careful solution will be given to against copyright infringement on file-sharing networks.

Keywords: encryption, copyright, privacy, file sharing

[*] Graduate School – National Economics University, Hanoi-Vietnam.

[**] Dean, Faculty of Law, National Economics University, Hanoi-Vietnam.

I. Introduction

File-sharing technologies have become popular in recent years, as a result of the cost reduction of storing and transmitting data.[1] This development benefits Internet users who upload and download files on the Internet, but also challenges copyright owners who face online piracy. To deal with this issue, right holders often request the file-sharing service providers to remove pirated contents and sometimes file a lawsuit against the piracy.

However, pirates could apply encryption to hide illegal copies from the seeking of copyright holders. The situation becomes worse when some hosting providers encrypt data automatically in an attempt to avoid their responsibilities for copyright infringement, facilitating the piracy and raising a new obstacle for the rights owners. On the other hand, encryption could be used properly to secure sensitive information, protecting the Privacy of users.

This article will clarify the conflict between Privacy of file-sharing users and the Intellectual Property right of content owners. This topic will be analyzed through 4 main sections of this article. Section II will give a definition of encryption. Section III will show the application of encryption in Privacy and Intellectual Property. Section IV will describe file-sharing models and point out the liabilities for copyright infringement of parties involved in file-sharing. Next, this paper will demonstrate how the encryption could be used by pirates and file-sharing service providers to avoid responsibility for copyright infringement. Two encrypting methods and their features will be clarified. After that, section V will propose some solutions to combat piracy, especially sharing encrypted content, but still appreciate the Privacy of users. Finally, a conclusion will be given with some main features.

II. Definition of encryption

Cryptography and encryption are two different terms and people sometimes confuse them. Thus, these two terms need to be clarified and distinguished.[2] A simple definition of cryptography is "*the design and use of communication schemes aimed at hiding the meaning of the message from everyone except the intended receiver.*"[3] Cryptography can use algorithms, protocols and strategies in order to protect sensitive information from

[1] Andrew Murray, INFORMATION TECHNOLOGY LAW, 39 (2nd ed. 2013).

[2] Bright Hub, Encryption vs. Cryptography-What Is The Difference?, May 26, 2015, http://www.brighthub.com/computing/enterprise-security/articles/65254.aspx (last visited July 13, 2015).

[3] Susan Loepp &William Kent Wootters, PROTECTING INFORMATION: FROM CLASSICAL ERROR CORRECTION TO QUANTUM CRYPTOGRAPHY, 1 (2006).

unauthorised access and it is not relay on computer science.[4] Cryptography includes 2 main processes: encryption and decryption.[5] Encryption or encipherment is a process which transforms a message (plain text) into coded version (cipher text). On the other hand, decryption or decipherment is the reverse of encryption, which recovers plain text from the cipher text.[6] It is clear that encryption is just one part of cryptography.

III. Applying encryption for Privacy and Intellectual Property

A. Applying encryption for Privacy

1. The right to Privacy

The right to Privacy is recognized as a fundamental human right by the United Nations (UN), under article 12 of Universal Declaration of Human Rights: "*No one shall be subjected to arbitrary interference with his Privacy…Everyone has the right to the protection of the law against such interference or attacks.*" Many countries in the world respect this right and adopt in national regulations to protect their citizens. In America, the Amendment IV of Bill of Rights states: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*." The EU also regulates the right to Privacy in article 8 of the European Convention on Human Rights: "*Everyone has the right to respect for his private and family life, his home and his correspondence.*" Through these regulations, the Privacy right is an important right and should be protected.

One aspect of Privacy is personal data Privacy, which refers to "*the collection, disclosure, and use of our personal information by known and unknown government and corporate entities.*"[7] Data Privacy is secured by many legislations such as Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such and the Data Protection Act 1998 in the UK. The Data Protection Act emphasizes the stronger protection for sensitive personal data in the article 2, including: the racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, whether he is a member of a trade union, physical or mental

[4] Keyvan Derakhshan Nik, CRYPTOGRAPHY, ENCRYPTION/DECRYPTION AND STEGANOGRAPHY, 4 INDIAN JOURNAL OF FUNDAMENTAL AND APPLIED LIFE SCIENCES 646 (2014).

[5] Rita Esen, *Cryptography And Electronic Data*, 2 THE NEW LAW JOURNAL, at 150 (2000).

[6] Alan G Konheim, COMPUTER SECURITY AND CRYPTOGRAPHY, 2 (2007).

[7] Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 Wm. & Mary L. Rev. 1501, 1509 (2015).

health or condition, sexual life and criminal records.[8]

2. The threat to data Privacy

In the digital era, personal data is normally saved in electronic forms such as email, Microsoft word, Excel, video, password and so on. However, the digital data could be seized without the will of information owner in 2 cases. In the first case, personal information is stolen illegally by hackers. Another case is personal data is collected legally by the government. In both 2 cases, the leak of personal data may harm to the live of victim in many aspects such as reputation, property and health.

Firstly, the personal data is a valuable target of cyber criminals on the Internet. According to Kimberly Kiefer Peretti, personal information such as social security number, bank account and credit card number could be stolen to commit identity-related crimes. Especially, criminals often sell the stolen financial information on "carding forums", the criminal websites like "Shadowcrew", allowing their members to exchange stolen personal data. The activity of this black market is complicated and worldwide.[9] Sometimes, the target of criminals is not financial information, but other sensitive information of victims. An example is the data breach of "Ashley Madison", a dating website, in July 2015. The hackers in "The Impact Team" obtain not only credit card details but also "*secret sexual fantasies*" of 37 million customers of "Ashley Madison".[10] The victims are worried about the public criticism, which can damage their reputations as well as their marriages. Furthermore, the criminals may use the secret to blackmail or manipulate the victims.

Secondly, personal data could be compiled by the government for some purposes such as national security or crime prevention. The surveillances are conducted legally and follow specific procedures. For example, in the US, 48 jurisdictions including the federal government, Puerto Rico, the District of Columbia, the Virgin Islands and 44 states authorize courts to order oral, wire and electronic interceptions.[11] The procedure of wiretapping is regulated in section 2518 of Title 18 of the United States Code. However, there are many concerns about the surveillances, although they are totally legal and used for

[8] *Data Protection*, GOV.UK, https://www.gov.uk/data-protection/the-data-protection-act (last visited Aug. 15, 2015).

[9] Kimberly Kiefer Peretti, *Data Breaches: What The Underground World of "Carding" Reveals*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 375, 375-376 (2008).

[10] *Ashley Madison Infidelity Site's Customer Data Stolen*, BBC News,.http://www.bbc.co.uk/news/technology-33592594 (last visited Aug. 16, 2015).

[11] *Wiretap Report 2014*, United States Courts, http://www.uscourts.gov/statistics-reports/wiretap-report-2014 (last visited Aug. 16, 2015).

good purposes. These concerns are reasonable: some powerful organizations like the NSA and the UK Government Communications Headquarters (GCHQ) are able to collect individual information without a strict procedure. For instance, the Foreign Intelligence Surveillance Court, which is so-called Fisa court, allows the NSA to collect data of the US citizens without a warrant.[12] For this reason, many Privacy supporters allege that the NSA abuses its power to violate the Privacy of billions of innocents in the world. This argument is emphasized by Kim Dotcom: "*the government's point of view might be: if you haven't done anything illegal, why would you care if the government captures all your data? My point of view is this: if I am not doing anything illegal, why has all my data been captured?*"[13] The government's surveillance sparks the angers from its targets and some people tries to against this activity. In *Jewel v. NSA* case,[14] the Electronic Frontier Foundation (EFF) on behalf of Carolyn Jewel and several other AT&T customers filed a lawsuit against the NSA in 2008 in order to "*stop the illegal unconstitutional and ongoing dragnet surveillance.*"[15] The district court dismissed the claims of the plaintiff because Jewel lacked standing. However, the court did not rule whether NSA collection program violated the Fourth Amendment.[16] There is another concern that the databases of government agencies are also the targets of hackers, which means personal information collected by the government could be breached. An example is the data breach from the United States Office of Personnel Management (OPM) in 2015. The OPM holds personal information of the US citizens including criminal records, histories of drug abuse, financial problems as well as fingerprints and uses these sensitive data to launch background investigations for over 100 federal agencies.[17] Thus, the leakage of OPM data affects to a huge number of people: up to 21.5 million victims.[18] For these reasons,

[12] Glenn Greenwald & James Ball, *The Top Secret Rules That Allow NSA to Use US Data Without A Warrant, the Guardian*, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant (last visited Aug. 16, 2015).

[13] Kim Dotcom, *Mega's EPIC Launch*, https://www.youtube.com/watch?v=LwlLC2PUrH8 (last visited Aug. 16, 2015).

[14] *Jewel v. NSA*, 673 F.3d 902 (2011).

[15] Electronic Frontier Foundation, *'Jewel V. NSA' (2011), https://www.eff.org/cases/jewel* (last visited Aug. 16, 2015).

[16] Dustin Volz, *Judge Dismisses Challenge to NSA Internet Surveillance*, http://www.nationaljournal.com/tech/judge-dismisses-challenge-to-nsa-internet-surveillance-20150210 (last visited Aug. 16, 2015).

[17] Background Investigations, U.S. Office of Personnel Management, https://www.opm.gov/investigations/background-investigations/ (last visited Aug. 16, 2015).

[18] Martyn Williams, *OPM Hackers Stole Data On 21.5M People, Including 1.1M Fingerprints, Computerworld*, http://www.computerworld.com/article/2946031/cybercrime-hacking/opm-hackers-stole-data-on

personal data Privacy is threatened seriously, as Richard Aldrich warned: "*we will soon have to live in a world with no such thing as Privacy and no such thing as secrecy.*"[19]

3. The role of encryption in Privacy

The threat to data Privacy comes from the technology and it also could be prevented by the technology. Encryption is one technological method to protect the personal information from the surveillance of government as well as criminals.[20]

Today, encryption is accepted in almost all countries in the world and there are many encryption programs which could be downloaded easily on the Internet. It means encryption becomes popular and the number of encryption users increases dramatically.[21] There is not anything wrong to encrypt the data to protect the right to Privacy, a fundamental human right. Because encryption is not only for the criminals, which are just a small part of the world, to conceal the sins, but also for billions of the innocents to shelter themselves from the risk of data breach.

Some people are concerned about the strength of encryption programs: could the government or hackers decrypt the cipher text easily? The answer of this question depends on the type of encryption. Even though it is true that: "*it is easier to encrypt information than it is to decrypt it*", according to Julian Assange, but the intelligence agencies may exploit the bugs on program to decrypt quickly. For instance, Microsoft has a policy that enables them to disclose the information about weaknesses in its programs to the US government.[22] Thus, choosing trusted encryption programs is important to ensure that the encryption providers cannot decrypt their products. Unfortunately, the users normally do not know which software do not include backdoors. Perhaps the free and open source software like Tor, LUKS, TLS and Open PGP are trusted, although they are not totally safe.[23]

-215m-people-including-11m-fingerprints.html (last visited Aug. 16, 2015).

[19] Katie Collins, *Espionage In A Post-Privacy Society*, May 20, 2014, http://www.wired.co.uk/news/archive/2014-05/20/espionage-after-the-loss-of-secrets (last visited Aug. 16, 2015).

[20] Daniel J. Sherwinter, *Surveillance's Slippery Slope: Using Encryption to Recapture Privacy Rights*, 5 J. Telecomm. & High Tech. L. 501, 504 (2007).

[21] *Id.* 524.

[22] Micah Lee, *Encryption Works: How to Protect Your Privacy In The Age of NSA Surveillance*, FREEDOM OF THE PRESS FOUNDATION, JULY 2, 2013, https://freedom.press/encryption-works (last visited Aug. 16, 2015).

[23] *Id.*

B. Applying encryption for Intellectual Property

Intellectual Property (IP) is built on the creation of mind and IP law protects some rights of owners such as reproduction and transmission. However, IP law is not enough to protect the creation of owners from the competitors in the market, especially in digital environment, the information can be copied easily.[24] Hence, encryption is a technological solution for the IP owners to prevent the leakage of trade secret and pirated copies.

1. Protecting trade secret

Generally, a trade secret is a confidential information that brings commercial value to its owner and it is kept secret.[25] Section 1839 of Title 18 of the US Code describes: "*the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.*" This section also imposes 2 requirements: the owner of information must use reasonable measures to keep it secret and "*the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.*"[26]

Through the definition above, the value of a trade secret depends on the protection of the owner. If the information is disclosed to the competitors, the owner lose his advantages in the market and therefore, this information will become worthless. The trade secret is a target of economic espionage and theft who steal it to benefit foreign government, foreign instrumentality, foreign agent or anyone other than the owner.[27] Today, the risk of trade secret disclosure is magnified by the Internet. According to Elizabeth A. Rowe, the Internet facilitates its users to post information including trade secret without any censorship and cause harmful effects to the owner. Additionally, the law

[24] Andrew Stranieri & John Zeleznikow, *Copyright Regulation with Argumentation Agents*, 10 Info. & Comm. Tech. L. 109 (2001).

[25] Francis J. Duffin & Bryan S. Watson, *Best Practices In Protecting and Enforcing Trademarks, Copyrights, and Other Intellectual Property Rights*, 28-WTR Franchise L.J. 132, (2009).

[26] Ronald D. Coenen Jr., Jonathan H. Greenberg & Patrick K. Reisinger, *Intellectual Property Crimes*, 48 Am. Crim. L. Rev. 849, 853 (2011).

[27] *Id.* at 854-855.

does not forbid the leakage from the third parties, who discover the trade secret and disseminate it on the Internet, as a judge comments: "*The anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation.*"[28]

As section 1839 mentions, the owner must apply reasonable measures to protect the trade secret. Joan M. Swartz points out some measures, including encryption software.[29] The encryption requires a proper password to access trade secret and normally just few people know this password. The encryption also can prohibit copying, scan and transfer the encrypted data.

2. Digital Rights Management

In copyright field, piracy is a big challenge for the copyright owner. Particularly, in the digital world, a content could be duplicated and distributed illegally without any cost on the Internet, resulting in huge amount of losses for copyright owners in many industries like music, video and game.[30] According to a research of the Institute for Policy Innovation, an annual loss for music piracy is about $12.5 billion in the US.[31] In game industry, piracy causes $3.5 billion of lost revenue per year in America and Canada, as the Entertainment Software Association (ESA) reports.[32] From these enormous numbers, it is clear that piracy harms seriously to the copyright owner and the economy.

Digital rights management (DRM) is a tool of copyright owner to prevent illegal copying. According to the OECD working party, one essential factor of DRM is encryption, which keeps the protected content unavailable to unauthorized users.[33] Florian Koempel classifies DRM into 2 groups: technological protection measures (TPM) and rights management information (RMI). Encryption falls into the first group.[34] In a general DRM model, the

[28] Elizabeth A. Rowe, *Saving Trade Secrets On The Internet*, 42 WAKE FOREST L. REV.1, 4-5 (2007).

[29] Joan M. Swartz, *Is It Safe? Is It Secret? Protecting Business Information*, GPSOLO 13 (2007).

[30] Chih-Ta Yen, Horng-Twu Liaw & Nai-Wei Lo, *Digital Rights Management System With User Privacy, Usage Transparency, and Superdistribution Support*, 27 INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS 1714, 1714 (2014).

[31] Who Music Theft Hurts (2012), http://www.riaa.com/physicalpiracy.php?content_selector=piracy_details_online (last visited Aug. 17, 2015).

[32] Peter Holm, *Piracy On The Simulated Seas: The Computer Games Industry's Non-Legal Approaches To Fighting Illegal Downloads Of Games*, 23 INFORMATION & COMMUNICATIONS TECHNOLOGY LAW 61 (2014).

[33] Catherine Stromdale, *The Problems with DRM*, 17 ENTERTAINMENT LAW REVIEW 1 (2006).

[34] Florian Koempel, *Digital Rights Management*, 11 COMPUTER AND TELECOMMUNICATIONS LAW REVIEW 239 (2005).

content is encrypted by the producer. After the content is purchased by the customer, a corresponding license is sent from the producer to the customer through the license broker. The customer uses the license to decipher the encrypted content.[35]

DRM is protected by anti-circumvention regulations, which prohibit the activities to avoid or disable DRM on the content. Article 11 of the WIPO Copyright Treaty (WCT) regulates that: "*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.*" Similarly, the article 18 of the WIPO Performances and Phonograms Treaty restates the protection of TPM. The EU adopts TPM protection in article 6 of the Information Society Directive. In the US, TPM circumvention is banned under section 1201 of Title 17 of the US Code: "*No person shall circumvent a technological measure that effectively controls access to a work protected under this title.*"

IV. Sharing encrypted data

A. The meaning of "file sharing"

"File sharing" is a common concept which emerged with the development of computer networks. Nowadays, the term "file sharing" describes the distribution or making available digital materials such as movie, music and photo to other users on the Internet.[36] However, the name "file sharing" is controversial and a question is raised: why is this term called "file sharing"?

According to the Oxford English dictionary, the origin of the verb "to share" appeared in the 16th century, meant "*division, part into which something may be divided*".[37] Base on this meaning, the name "file sharing" could be a misnomer, because the distributor does not lose anything when he transfers a file to a receiver. Richard Parsons, the CEO of Time-Warner states: "*it isn't sharing, it's online shoplifting.*"[38] From this point of view, some copyright owners try to refer "file sharing" to online piracy and criticize that file sharing

[35] Yen et al, *supra* note 30, at 1716.

[36] *What Is File Sharing?*, UC San Diego, http://acms.ucsd.edu/filesharing/general.html (last visited Aug. 18, 2015).

[37] Oxfordlearnersdictionaries.com, '*Share Verb'*, http://www.oxfordlearnersdictionaries.com/definition/english/share_1#share_1__4 (last visited Aug. 18, 2015).

[38] Jessica Litman, *Sharing and Stealing*, 27 Hastings Comm. & Ent L.J. 1 ,23 (2004).

networks are the tools for piracy.

From another approach, "file sharing" is similar to "sharing idea". When an idea is widespread, the generator still remembers it.[39] Perhaps this opinion is more relevant because the concept of "file sharing" bases on "perfect copies", which means the digital content is reproduced exactly without any cost. After the reproduction, a copy is sent to another person while the original file is still kept by the creator.[40] With this progress, the content can be distributed to an unlimited number of people.

According to Nicholas John, there are 2 main ways to share the data: via physical media like flash memory and external hard disk drives, or via computer networks. In both 2 ways, file sharing appeared in few decades ago. For example, traced back to 1971, people used File Transfer Protocol (FTP) and IBM floppy disk to transfer the data.[41] However, the term "file sharing" just became popular in 1999 with Napster, a peer-to-peer (P2P) network.[42]

B. Types of file sharing networks

There are several models of file sharing networks such as Local Area Network (LAN), FTP, P2P, email and file hosting service.[43] Among them, P2P and file hosting service are the 2 most popular methods which facilitate the sharing between many participants in these networks.

1. P2P network

According to Ion Stoica, P2P networks "*are distributed systems without any centralized control or hierarchical organization, in which each node runs software with equivalent functionality.*"[44] From this definition, a standout feature of P2P network is pointed out by Markus Hofmann and Leland R. Beaumont that because of the equality between peers, each peer can change its role in P2P system such as client, server, network as well as router. Beside the pure P2P network, the hybrid P2P system can apply hierarchical and centralized

[39] *Id.*

[40] Graham Dutfield & Uma Suthersanen, *GLOBAL INTELLECTUAL PROPERTY LAW*, 234 (2008).

[41] Nicholas A. John, *File Sharing and The History of Computing: Or, Why File Sharing Is Called "File Sharing"*, 31 CRITICAL STUDIES IN MEDIA COMMUNICATION 198, 203 (2014).

[42] Stan J. Liebowitz, *File-Sharing: Creative Destruction Or Just Plain Destruction?*, 49 J.L. & Econ. 1 (2006).

[43] Bradley Mitchell, *The Beginner's Guide to Network File Sharing* (2007), http://compnetworking.about.com/od/basicnetworkingconcepts/a/file_sharing.htm (last visited August 18, 2015).

[44] Ion Stoica et al., *Chord: A Scalable Peer-To-Peer Lookup Protocol for Internet Applications*, 11 IEEE/ACM TRANSACTIONS ON NETWORKING 17, 17 (2003).

resources.[45]

P2P networks are divided into 3 generations in chronological order, with different characteristics. The first generation is centralized P2P model and a notable is Napster. Napster was created in 1999 by Shawn Fanning as a music network allowing users to locate and download unprotected songs. Napster had a central server and its function is just introducing the client to a host. A music file was located in the host and it was transferred directly from the host to the client, not through Napster central serval.[46] Thus, Napster did not contain, copy nor create any song on its server. In July 2001, Napster was close down after it was charged with contributory infringement and vicarious infringement in *A&M Records, Inc. v. Napster, Inc.* case.[47]

After Napster, the second generation P2P networks were developed without a central server. There are 2 models: decentralized P2P and semi-structured P2P. In decentralized system, a new member participates in the network by a nearest active node. Every request is forwarded through the network. For example, node A needs a song and asks node B. Node B does not have this song, but it asks node C. If node C has this song, it will connect to node A and transfer this song. If Node C does not, it will pass this request to other nodes. Thus, the number of peers which involve to implement a request could be big, resulting in a huge amount of network traffic as well as slow speed. Another model in the second generation is semi-structured P2P, which combines the features of both centralized and decentralized types. Although semi-structured P2P also does not use a central server like decentralized system, its speed could be faster than decentralized model, because it chooses some temporary information host called super-node to execute requests. For instance, node A, B and C are in a group and node A is a temporary host, who keeps the detail of his group in a list. Node B asks node A for a song, node A will check his list. If A finds that C has this song, he will invite B to C to communicate. If no one in his group contains this song, node A will ask other hosts of other groups. Some notables of the second generations are Grokster, Kazaa, Morpheus, EDonkey and Gnutella.[48]

The third generation is BitTorrent, which is completely different to 2 previous P2P generations. BitTorrent is faster than the older P2P because the file is broken up into small segments and downloaded from multiple people also hosting these pieces.[49] For example, computer A needs a movie which is

[45] Markus Hofmann & Leland R. Beaumont, CONTENT NETWORKING: ARCHITECTURE, PROTOCOLS, AND PRACTICE (THE MORGAN KAUFMANN SERIES IN NETWORKING) 148 (2005).

[46] Murray, *supra* note 1, at 266.

[47] *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

[48] Murray, *supra* note 1, at 271-272.

[49] Natasha Culzac, *What Is Bittorrent? A Short Description of The File Sharing Protocol...* ,

divided into 100 fragments and contained by computer B, C and D. B is a seeder, who keeps full parts of the movie, whereas C and D are leechers keeping 30 and 60 parts respectively. A, B, C and D join a "swarm" to share what they have to each other. A will download from B, C and D; C will download from B and D; D will download from B and B will just upload. With this protocol, BitTorrent facilitate users to download large files with minimum Internet bandwith.[50] To use BitTorrent protocol, users must download a BitTorrent client, a computer program, such as µTorrent, Xunlei and Vuze. The client downloads and upload BitTorrent files containing metadata of movie. A well-known BitTorrent index is the Pirate Bay, a Swedish website, which lists available Torrent files.[51]

2. File hosting service

Compare to P2P networks, file hosting service or cloud storage service is totally different. The users upload files to a space (host) through a web interface and they can manage and share files after that. Files are served in the host with a specific address. A unique link is generated for a file and people use this link to access the address of file and download it.[52] Sometimes, a file could be protected by a password and only permitted people who know the password can download it. Some popular cloud storage services are Google Drive, Dropbox, Microsoft One Drive, Mega and Apple iCloud.[53] In general, cloud storage services divide customers in 2 groups: premium users and free users with different policies. While free users are restricted in downloading numbers, file sizes, waiting time as well as downloading speed, the services facilitate the download of premium customers and give them other supports. With this discrimination, the service providers persuade users to pay premium fee to receive advantages, especially who need to download or upload large files frequently.[54]

INDEPENDENT, http://www.independent.co.uk/life-style/gadgets-and-tech/news/what-is-bittorrent-a-short-description-of-the-file-sharing-protocol-9758805.html (last visited Aug. 19, 2015).

[50] Mark Scanlon, Jason Farina & M-Tahar Kechadi, *Network Investigation Methodology for Bittorrent Sync: A Peer-to-Peer Based File Synchronisation Service*, 50 COMPUTERS & SECURITY 3 (2015).

[51] Murray, *supra* note 1, at 276.

[52] Aniket Mahanti et al., *Characterizing The File Hosting Ecosystem: A View from the Edge*, 68 PERFORMANCE EVALUATION 1085 (2011).

[53] Martyn Casserly, *The Best Cloud Storage Services: Dropbox vs Google Drive, Onedrive, Icloud & More*, http://www.pcadvisor.co.uk/test-centre/internet/13-best-cloud-storage-services-2015-3614269/ (last visited Aug. 19, 2015).

[54] Mahanti, *supra* note 52, at 1085.

The main point of file hosting service is keeping file in the central location, not in HDD of members like P2P. This feature brings both advantages and disadvantages to the users. Users can back-up their data on the cloud and restore or access data in other devices like tablets and mobile phones anywhere, which is so-called "always-on" access. Some cloud services like Google Drive allow users to open online some kinds of files like Microsoft Word without download. Thus, users do not waste the space of their device to keep a copy.[55] Furthermore, because a file is downloaded directly from a host, so the downloading speed does not depend on the Internet speed of the uploader like in P2P system. Practically speaking, the uploading speed is much slower the downloading speed.[56] Thus, the cloud users are able to download with faster speed than in P2P. Moreover, people sometimes want to download rare files, which are contained in few places. However, in P2P network, people only can download rare files when the uploader is online. In contrast, people can download from the host anytime even if the original uploader is offline.[57]

Beside these pros, the cloud storage services also have some drawbacks. In some cases, files are deleted by the service providers because of copyright infringement or unlawful content. The data also could be lost if the server is shutdown. An example is the close of Megaupload in 2012. Megaupload was seized suddenly without any notice by the United States Department of Justice (DOJ). Even though Megaupload refused to delete the data of customers, but it is difficult for users to retrieve their files.[58] Another concern is the security of hosting services. The services could be attacked by the hackers from vulnerabilities and the data could be destroyed or stolen. Resisting the attack is not simple because: "*cloud security is a complex issue influenced by many factors and choices including: solution architecture, service model, deployment model, and hosting environment.*"[59]

C. Liability for copyright infringement

Involving in file sharing, there are 3 main parties: the uploaders, the downloaders and the online service providers (OSP) including P2P provider and

[55] Scanlon, *supra* note 50, at 3.

[56] Chris Marling, *How Fast Is My Broadband? A Guide to Upload Speed, Download Speed and How to Check It - Broadband Ge*, https://www.broadbandgenie.co.uk/broadband/help/how-fast-is-my-broadband-upload-speed-download-speed-and-speed-test (last visited Aug. 19, 2015).

[57] Richard Abbott, *The Reality of Modern File Sharing*, 13 J. INTERNET L. 3, 3 (2009).

[58] Electronic Frontier Foundation, *Megaupload Data Seizure*, https://www.eff.org/cases/megaupload-data-seizure (last visited Aug. 19, 2015).

[59] Edit Szilvia Ruboczki & Zoltan Rajnai, *Moving Towards Cloud Security*, 13 INTERDISCIPLINARY DESCRIPTION OF COMPLEX SYSTEMS 9, 11 (2015).

hosting provider (the definition of OSP is written in section 512(k)(1) of title 17 of the US Code). While the number of downloaders is numerous and unidentified, the number of uploaders is much smaller. More importantly, from sharing pirated copies of movies, music and games, the uploaders and the OSP can obtain economic benefit[60] whereas the downloaders just want to entertain themselves. Thus, the copyright owner and the government often allege the uploaders and the OSP in copyright infringement cases.

1. Direct infringement

The direct copyright infringement happens when a person commits some activities without the permission of copyright owner.[61] There activities are given in section 106 of title 17 of the US Code, including: "*to reproduce the copyrighted work in copies or phonorecords*" and "*to distribute copies or phonorecords of the copyrighted work to the public.*" Thus, the uploaders who make and share pirated copies on the Internet are responsible directly for copyright infringement. For instance, a man in the UK who uploaded illegally the World Wrestling Entertainment (WWE) and the Ultimate Fighting Championship (UFC) was arrested by the Police Intellectual Property Crime Unit (PIPCU). These copies were downloaded 2 million times and resulted in millions of pounds in lost revenue for the copyright owners.[62]

Unlike the pirated uploaders who are clearly liable for direct infringement, it is difficult for the copyright owners to claim the direct infringement to the OSP, although the pirated copies are processed automatically by the OSP networks. An example is *Disney Enterprises, Inc. v. Hotfile Corp.* case.[63] Hotfile is a hosting service allowing its users to upload and download files. When a file is uploaded, the server makes 5 additional copies and generates a unique link for each copy. Disney claimed that the defendant violated the reproducing right, an exclusive right of the copyright owner under section 106 of title 17 of the US Code. However, the district court disagreed with plaintiff's argument because the automatic copying conducted by software is not volitional. Therefore, the court held that Hotfile was not liable directly for copyright

[60] Calum Darroch, *Problems and Progress in The Protection of Videogames: A Legal and Sociological Perspective*, 1 THE MANCHESTER REVIEW OF LAW, CRIME AND ETHICS 136, 157 (2012).

[61] Direct Infringement | Wex Legal Dictionary / Encyclopedia | LII / Legal Information Institute, https://www.law.cornell.edu/wex/direct_infringement (last visited Aug. 20, 2015).

[62] *Man Arrested over Pirating of 3,000 WWE Wrestling Bouts*, Mar. 18, 2015, http://www.bbc.co.uk/newsbeat/article/31940270/man-arrested-over-pirating-of-3000-wwe-wrestling-bouts (last visited Aug. 20, 2015).

[63] *Disney Enterprises, Inc. v. Hotfile Corp.*, 798 F.Supp. 2d 1303 (S.D. Fla. 2011).

infringement.[64]

2. Secondary liability

A secondary liability or indirect infringement is derived from the primary liability, including 2 kinds: contributory infringement and vicarious infringement. A contributory infringement occurs when the third party has the knowledge about infringing activity and induces or materially contributes to the infringement. A vicarious infringement arises when the third party has a direct financial benefit from infringement and has the right as well as ability to control the actions of the direct infringer but fails to stop these unlawful actions.[65]

The OSP may take secondary liability for copyright infringement. In *Perfect 10, Inc. v. Megaupload Ltd.* case,[66] the defendant was charged with contributory infringement. The plaintiff, Perfect 10, was an adult websites creating pornographic photographs, videos and magazines. However, their products were uploaded illegally to Megaupload by users. The links of pirated contents were disseminated by Megaupload and its users on the Internet. Especially, Megaupload provided substantial payouts to affiliate websites which catalogued the pirated links. Furthermore, Megaupload offered a reward program to the uploaders in order to increase the downloading number. In spite of receiving 22 infringing notices from the plaintiff, Megaupload did not remove pirated contents. Based on these facts, the court held that Megaupload was a contributory infringer because 2 requirements were met. Firstly, the defendant had the knowledge about infringement from 22 notices and the act of affiliate websites. Secondly, through substantial payouts and reward program, Megaupload induced or materially contributed to infringing conduct. Nonetheless, the defendant was not liable for vicarious infringement in this case, because it did not have ability to supervise infringing conduct. Unlike in *A&M Records, Inc. v. Napster, Inc.* case,[67] where Napster P2P network required its users to register and log in, the Megaupload users just needed the links to access and download without registration and login. For this reason, Megaupload could not terminate users' access.

[64] Mary Rasenberger & Christine Pepe, *Copyright Enforcement And Online File Hosting Services: Have Courts Struck The Proper Balance?*, 59 J. COPYRIGHT SOC'Y U.S.A. 627, 636 (2012).

[65] Christian E. Mammen, *File Sharing Is Dead! Long Live File Sharing! Recent Developments In The Law Of Secondary Liability For Copyright Infringement*, 33 Hastings Comm. & Ent L.J. 443, 447 (2011).

[66] *Perfect 10, Inc. v. Megaupload Ltd.*, No.11-CV-00191 (S.D. Cal. July 27, 2011).

[67] *Supra* note 47.

D. Encrypting pirated data to avoid responsibility for copyright infringement

Both pirated users and OSP could be liable for copyright infringement. To avoid their responsibilities, encryption is an effective tool, which protects not only Privacy and security, but also piracy.

From the perspective of pirates, encryption can prohibit the access to the content. Hence, the copyright owners could not know whether the data is pirated or not if they do not seize the password. Additionally, encrypted files can avoid the filtering of the OSP. It is noticed that the OSP applies some programs such as deep packet inspection (DPI) to identify and block or remove the known illegal files. Each file contains an exclusive hash value. The hash value of pirated data is listed and the DPI recognises and prohibits files in this list. However, the DPI is unable to scan encrypted data to know its hash value.[68]

The encryption also brings advantages for the OSP who is reluctant to remove and block pirated files on their networks. If the OSP cannot identify the encrypted pirated copies, it does not have knowledge about the infringing conduct and cannot stop the action of direct infringer. Therefore, the OSP could evade the secondary liability for copyright infringement. However, this argument is controversial. The copyright owners argue that applying encryption may lead to willful blindness, which means avoiding liability "*by intentionally putting oneself in a position to be unaware of facts which create liability.*"[69] For example, in *In re Aimster Copyright Litigation case*[70], the defendant, Deep, encrypted songs which are shared via Aimster P2P system to avoid knowledge about infringing acts of his users. The court ruled that: "*a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used.*" Thus, the defendant was held liable for contributory infringement.

In contrast, the hosting provider argues that it could get plausible deniability, which means "*a denial of responsibility or knowledge of wrongdoing cannot be proved as true or untrue due to a lack of evidence proving the allegation.*"[71] This protection is given in section 512(c)(1)(A)(i) of title 17 of the US Code (the Safe Harbor for the hosting provider): "*a service provider shall not be liable infringement of copyright by reason of the storage*

[68] Abbott, *supra* note 57, at 6.

[69] *Willful Blindness Law & Legal Definition*, Definitions.uslegal.com, http://definitions.uslegal.com/w/willful-blindness/ (last visited Aug. 21, 2015).

[70] *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003).

[71] *Plausable Deniability Law & Legal Definition*, USLEGAL, http://definitions.uslegal.com/p/plausable-deniability/ (last visited Aug. 21, 2015).

at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider does not have actual knowledge that the material or an activity using the material on the system or network is infringing."

E. Encrypting methods

In general, there are 2 ways to encrypt the data: client-side encryption and shared-key encryption. Each method has some special features and affects to the users and the OSP.

Firstly, the users can encrypt the data prior to sharing by using encipherment software. The data is encrypted on the computers of users and thus, the OSP cannot know the keys as well as contents (zero-knowledge). However, before using this method, the users must trust the software developer. If there is a backdoor on the program, the data could be unauthorized decrypted easily.[72] There are various encryption programs such as Boxcrypto, Ensafer and SharedSafe supporting online storage for the users.[73] Some file hosting providers such as Mega and SpiderOak apply client-side encryption. The P2P users also can encrypt data manually before sharing. With client-side encryption, the users highly secure their Privacy and the OSP with zero-knowledge can obtain plausible deniability to refuse their liability for copyright infringement. However, if the key is lost, it is nearly impossible to recover the data.[74]

The second method, shared-key encryption, is totally different. All files are encrypted after they are stored in the host with a single key. It means the hosting providers know the key and they can decrypt to view the contents. It seems that shared-key encryption just protects data from the attacks of hackers rather than the Privacy of users. The reason of the hosting providers for applying this method is deduplication. The OSP scans the hash values of unencrypted files before uploading to server and recognises which files have already been stored. Hence, the providers just need to keep a limited numbers of each data and save the space storage. If files are encrypted before uploading, the OSP could not examine the hash values and fails to avoid data repeating.[75] A small advantage

[72] Andrew Froehlich, *Zero-Knowledge Cloud Storage: Far From Perfect,* Network Computing, http://www.networkcomputing.com/cloud-infrastructure/zero-knowledge-cloud-storage-far-from-perfect/a/d-id/1319158 (last visited Aug. 22, 2015).

[73] Subrata Kumar Das and others, *Performance Analysis of Client Side Encryption Tools*, 4 INTERNATIONAL JOURNAL OF ADVANCED COMPUTER RESEARCH 888, 888 (2014).

[74] Froehlich, *supra* note 72.

[75] *Slight Paranoia: How Dropbox Sacrifices User Privacy for Cost Savings*, PARANOIA.DUBFIRE.NET, http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-Privacy-for.html (last visited Aug. 22, 2015).

of this method for the customers that they do not need to upload a data again.[76] Some popular hosting services using shared-key encryption are Dropbox, Google Drive and Microsoft OneDrive.

V. Solutions

Sharing encrypted data is a challenge for the copyright owners to attack online piracy in both technological and legal battles. On the other hand, the Privacy of the users also needs to be appreciated. The conflict between copyright owners and cryptographic users is not easy to be resolved, but the situation will be improved if there is a cooperation between multiple parties.

A. Notice and takedown pirated contents

Section 512(c)(1)(C) of title 17 of the US Code requires the hosting providers to remove or disable access to pirated contents when receiving notification of claimed infringement. The notification includes: "*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.*"

Based on this regulation, the copyright owner needs to find out the link and password of pirated content to notice the OSP about infringement. Normally, the owners can find the link and password which is posted on pirated websites and blogs. However, files could be shared in a secret group of people and not be widespread. In practice, the copyright owners focus on popular websites and blogs which are viewed by many people, rather than a small group including several members.

B. Shut down pirated websites and blogs

The next step of copyright owners is attacking websites and blogs which share copyrighted contents. Instead of enforcing numerous pirated uploaders and downloaders, it is more effective to target at administrators of these sites.[77] The Internet users often search links on popular websites, so if pirated websites

[76] Kai He et al., *Public Auditing for Encrypted Data with Client-Side Deduplication in Cloud Storage*, 20 WUHAN UNIVERSITY JOURNAL OF NATURAL SCIENCE 291, 291 (2015).

[77] Lucy England, *Police Have Raided the Most Popular Pirate Streaming Site in Sweden and Are Forcing It to Shut Down*, July 29, 2015, http://uk.businessinsider.com/sweden-pirate-streaming-site-swefilmer-shut-down-police-raid-2015-7 (last visited Aug. 22, 2015).

are taken down, people could not get pirated links, at least in a short time. However, other pirated websites may replace closed ones after that. Overall, this method just reduces piracy in a short period if only one site is blocked.[78]

To stop a website and arrest its administrators, an international cooperation is needed. Unfortunately, the conflict between national laws is a barrier for law enforcement. In some countries such as Switzerland, the copyright regulation is not strict. For example, article 19 of the Federal Act on Copyright and Related Rights permits "private use": "*Published works may be used for private use. Private use means: any personal use of a work or use within a circle of persons closely connected to each other, such as relatives or friends.*" This means a person is permitted to download copyrighted contents from every source whether it is legal or not. In the Annual Special 301 Report on Intellectual Property Rights 2015, the US Trade Representative criticizes that domestic environment creates "*a safe haven for piracy on the Internet*"[79]

C. Filtering hash value before encrypting

As mentioned above, there are 2 ways of encryption: client-side encryption and shared-key encryption. One technology which is applied by shared-key hosting providers like Dropbox is hash value filter, which can be used to recognize copyrighted content. Therefore, this function should be applied in every cryptographic programs to detect the hash value of file before encipher a file. The blacklist of hashes could be sent to software developers to adopt in their programs. If the filter identifies a pirated content, the software should refuse to encrypt this content. If the content is original, it will be encrypted.

It is noticed that hash identifier does not violate the Privacy of users although it scan the file. Firstly, the filter does not read the content of file and does not know what this content is. Thus, this filter does not know the sensible information of users. Assuming that a hash value is a fingerprint and it is used to identify a person. But a fingerprint cannot show the detailed information such as age, occupation or characteristic. Secondly, the hash value is irreversible. This means if someone collects this value, he cannot create a copy of file.[80]

To apply this method, a hash value database is necessary. Hash values are contributed by copyright owners to protect their products. A sample database is

[78] Torrent Freak, *Shutting Down Pirate Sites Is Ineffective, European Commission Finds*, https://torrentfreak.com/shutting-down-pirate-sites-is-ineffective-european-commission-finds-150514/ (last visited Aug. 22, 2015).

[79] United State Trade Representative, Annual Special 301 Report On Intellectual Property Rights (2015) at 18.

[80] *An Illustrated Guide to Cryptographic Hashes*, UNIXWIZ.NET, http://www.unixwiz.net/techtips/iguide-crypto-hashes.html (last visited Aug. 23, 2015).

the National Software Reference Library (NSLR), a collection of software hash values, established by the National Institute of Standards and Technology, an agency of the U.S Department of Commerce.[81]

VI. Conclusion

The encryption plays a vital role in both Privacy and Intellectual Property. Facing many threats to data Privacy from hackers and government, encryption is a shield to protect sensible data and also the lives. However, the strength of the encryption is questioned under a concern that the government can exploit the backdoors on programs. Thus, the open-source independent encryptions are encouraged to use. In the context of Intellectual Property, the encryption is used to protect trade secrets which are valuable targets of economic espionage and theft. Additionally, the encryption is applied in Digital Right Management to protect copyrights from online infringements.

Besides these benefits, the encryption also raises the conflict between Privacy and copyright in the digital environment. With the development of technology, file-sharing via peer-to-peer networks and hosting services becomes popular and is used to transfer copyrighted contents by piracy. The encryption is an obstacle for the right holders to seek illegal links, which require appropriate passwords to decipher. Furthermore, the encryption disables the file identifier and hides the hash value of data. In contrast, the encryption facilitates the piracy and the service provider, protects them from the liability for copyright infringement.

Facing this situation, it is necessary to apply some solutions to against online piracy, with the requisite is the Privacy of users must not be violated. Two common methods could be used are notice and takedown pirated contents as well as shut down pirated websites and blogs. Moreover, to dealt with encryption challenge, filtering hash value before encrypting may stop the abuse of encryption for piracy while the data Privacy is still secured.

[81] *Library Contents*, NSRL, http://www.nsrl.nist.gov/Library_Contents.htm (last visited Jan. 2, 2016).