Eric Li

Professor Eiselt

ECS 188 001

May 26, 2020

Word count: 1979

Ethical problems in P2P architectures

Peer-to-Peer (P2P) is a famous computer network architecture in contrast to the client-server architecture. Instead of relying on an always-on server to handle all requests, P2P applications communicate with other application users, which better utilizes the network's connectivity and alleviates burden on the server's traffic, increasing the overall speed [1]. P2P architecture became popular with a file sharing system called Napster in 1999 [2]. After a few decades' development, P2P now has popular applications in file sharing, software distributing, and anonymous browsing. However, this powerful technology has created ethical problems. Since P2P allows users to share files easily, people share more and more illegal data like pirated music and movies with this technology. Annoyed about the copyright infringement, the copyright holders try to monitor the sharing of pirated content, which creates concerns on P2P users' privacy. P2P also creates minor issues like leeching - utilizing P2P network's resources without reciprocating.

When sharing files, P2P systems have a large advantage compared to the traditional client-server systems. It is self-scalable when multiple peers are trying to download from a single server: the server's bandwidth is no longer the bottleneck of the system because the Internet connections between peers can be fully utilized. Another feature is that if the server goes down during the transmission, the remaining peers can possibly reconstruct the transmitted file using what they have already received [1]. However, this powerful downloading capability makes P2P

notorious for downloading pirated content. A technical report in 2011 estimates that 11% of all the Internet's traffic is infringing content on BitTorrent, a popular P2P protocol used for file sharing [3]. In order to understand this trend, there has been studies on the ethical choices people make when deciding whether to share infringed content through a P2P network. People realize the fact that downloading infringed content is an ethical issue. However, if they pay a subscription fee to use the P2P network, they feel less guilty or do not think they are pirating [4]. Peoples' beliefs in consumer rights let them download infringed content in P2P networks. Their beliefs in reciprocity let them decide to further share what they have downloaded to others [5].

The structure of the P2P file sharing network makes it difficult to stop the infringement. Unlike pirating hard-copied books or distributing the infringed content in a client-server manner, which can be stopped simply by cutting the sharer off, P2P networks are difficult to stop because essentially every user is a sharer. Copyright owners tried to protect their content by banning P2P technology because a blanket ban would be much easier to implement than tracking down and suing infringing individuals [6]. However, is it worthwhile to ban a technology just because of its potential damage to the copyright law? This move was not unprecedented as copyright owners tried banning the Sony Betamax recorder in 1984 because the home video system provided a way for people to make not only home videos but also copies of copyrighted materials [7]. However, the Supreme Court decided that Sony was not behaving illegally when developing, selling, and advertising the new video recorder. This ruling has since become known as the Sony Doctrine, and applies to developing and selling technologies that have large potential uses and commercial value. The judges' reasoning was that if the law does not provide such a safe harbor for technology developers, there will be a chilling effect on innovation. However, this ruling does not provide protections if the technology designers actively promote using their technologies for infringing on

copyrights. The P2P technology, under this analysis, is also legal because the technology is neutral and has significance in non-infringing uses [7].

To still stop the infringement without taking P2P systems down, copyright holders and the research community have thought of different ways and result in a polarized debate. Some people focus on building a system that resolves P2P copyright disputes [6]. Their main focus is to let each side provide evidence so that clear cases can be resolved easily. They propose that for repeated violations, there should be some harsh penalties like denial of Internet service. However, people on the other side have different opinions. They believe copyright owners should educate the customers about the immorality of piracy and persuade them to decline piracy, instead of simply enforcing the law [4]. They also propose that copyright owners should change their business models to make use of the P2P technology [5]. Researchers in the middle think P2P architecture decreases the distance between the authors and the public and facilitates the distribution of information in a desired way. Some actions like infringing should be considered immoral, but copyright holders should consider changing their way of sharing and protecting their copyright [8].

Letting copyright holders change and integrate into the P2P sharing nature seems unrealistic in the short term. So they implement different ways to stop infringement. To download a large file from BitTorrent, users need to first obtain a small torrent file from another website in order to find the large file in the network. Then they need to connect to tracker servers to find peers. Copyright owners ask search engines like Google to take down URLs that host torrent files for pirated content. They also try to take down trackers for infringing content so that users cannot find peers for downloading the file. Apart from taking down those servers, copyright owners directly monitor P2P users, which raises privacy concerns. Though P2P architecture becomes popular because of its "principles of anonymity and freedom," it turns out that in some ways monitoring users in P2P

networks is even easier than in client-server networks [9]. Wolchok et al. showed in 2010 that by crawling DHT, a data structure used by BitTorrent for tracking, they can track nearly 8 million IP addresses' downloads [10]. There are also websites that allow users to lookup download records of any IP address [11, 12, 13]. For copyright owners, an IP address can be mapped to an Internet user through a subpoena to the IP address' Internet Service Provider (ISP), though there may be some false positives caused by sharing of one IP address between multiple users [6]. So have governments or copyright holders actually monitored P2P users' activities? An experiment in 2007 shows that the government and trade associations like Recording Industry Association of America (RIAA) and Motion Picture Association of America (MPAA) are creating fake users in P2P networks for surveillance [14]. RIAA and MPAA are committed to protect the copyright for artists, but they do not address the problem of P2P users' privacy [15, 16]. As a way to protest, P2P communities have detected these fake IP addresses and published blocklists for P2P users. The 2007 experiment shows that if P2P users ignore the blocklist, they are almost always tracked by the government and the organizations. Now, there are still active research in P2P monitorization and anonymization using all kinds of techniques.

Due to the distributed nature of the P2P structure and the difficulties in administration, this new technology even directly and indirectly brings troubles to ISPs. In client server structure, users usually have more downloading traffic than uploading, but for P2P applications, downloading and uploading traffic are ideally the same. This contradicts many ISPs' design of asymmetric bandwidth, which is the direct trouble for ISPs [1]. The indirect trouble comes from the Digital Millennium Copyright Act (DMCA) enacted in 1998 [17]. The intention of this act is to prevent online service providers (OSPs) from being liable for users' infringing behavior. However, this safe harbor for OSPs requires them to follow the "notice and take down" policy. For an ISP, that means

when an infringement notice is received, the ISP has to quickly remove the source of infringement from the service. Many ISPs complain about this policy because they have to invest time and money on processing the notices [18]. Universities, who provide Internet service to their students, have to treat this problem more seriously. Unlike other ISPs, most Internet users in universities are students, so the universities have to regulate the students' conduct [18]. The Higher Education Opportunity Act in 2008 requires universities to notify students annually about their responsibilities on preventing infringement [19], and such kinds of notices can be easily found on many universities' websites [20, 21, 22]. As a disciplinary action, universities remove students in violation of DMCA from the campus network for a short period of time. In UC Davis, for example, it is 14 days. However, a survey shows that many universities have not registered an agent for processing the infringement notices, and the agents still need to properly understand the law related to DMCA [18]. Thus, P2P is bringing ISPs and universities troubles even though they have no direct relationship with the technology.

The idea of P2P sharing is that users can download what they need from the network, and in return, they should voluntarily provide what they have to other users, forming a reciprocal model. However, due to the open nature of the P2P protocol, users may configure their P2P clients so that they upload little or none to the network while still downloading the files successfully, known as leeching [23]. Some people's motivation for leeching is to save their bandwidth, and most people believe it breaks the P2P etiquette and is an unethical behavior. However, others have a different motivation for leeching, which comes from the ironic fact about the enforcement of DMCA that only uploaders are liable for the infringement, not the downloaders. Normally P2P users are accused of DMCA violation because by the default configuration of P2P agents, they upload the infringed content they have downloaded back to the P2P network for other peers. If a user leeches

by downloading the pirated content using a P2P network without uploading, he or she will not be accused of DMCA violation. It becomes another ethical question of whether to leech if the intention of leeching is to prevent the liability for DMCA violations (not considering whether pirating is ethical) [24].

Another ethical concern is about Xunlei's development on top of P2P networks that does not follow an open nature and the idea that P2P systems "must not have centralized control" [25]. Xunlei is a popular P2P application that operates on a proprietary network that shows centralized control. Worrying about the effect of centralized control on performance, privacy, and security, researchers try to reverse engineer Xunlei's network and compare its behavior to open P2P implementations. Their research shows that some requests Xunlei clients make are weakly encrypted, which allows attackers to see what other people download. It also shows that Xunlei's network is trying to "wrap" the other popular P2P networks. Though this practice may possibly make filtering infringement easier, it can easily monitor too many users' activities and harm privacy.

P2P is an influential technology in computer networks for applications like file sharing. But as Neil Postman mentions in his 1998 speech, this powerful technology does not distribute its advantage equally to all people [26]. It allows consumers to access pirated content easier, thus paying less to watch movies or listen to music. But it brings copyright holders and ISPs a nightmare. Copyright holders have to think of different ways to stop piracy on the P2P network, and ISPs have to invest time and money to deal with infringement notices. Moreover, as Postman mentions, P2P also has trade-offs on its users. Though they can download content easier, they have to share their bandwidth and may be monitored by the government and copyright holders. P2P also creates problems like leeching and construction of proprietary networks on top of it. There are more problems to be discussed, like the distribution of software updates over P2P by default and the

distribution of malicious files. Hopefully ethics can guide people to reach a solution to those problems in the future.

References

[1] James F Kurose. *Computer networking : a top-down approach*. eng. 6th ed. Boston: Pearson, 2013. ISBN: 9780132856201.

[2] Tom Lamont. *Napster: the day the music was set free*. Feb. 2013.

[3] Betjeman House. "Technical report: An estimate of infringing use of the internet". In: *Analysis* (2011), pp. 1–56.

[4] Connie Bateman, Sean Valentine, and Terri Rittenburg. "Ethical Decision Making in a Peer-to-Peer File Sharing Situation: The Role of Moral Absolutes and Social Consensus". In: *Journal of Business Ethics* 115 (June 2012). DOI: 10.1007/s10551-012-1388-1.

[5] Rong-An Shang, Yu-Chen Chen, and Pin-Cheng Chen. "Ethical Decisions About Sharing Music Files in the P2P Environment". In: *Journal of Business Ethics* 80 (Feb. 2008), pp. 349–365. DOI: 10.1007/s10551-007-9424-2.

[6] Mark A Lemley and R Anthony Reese. "A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes". In: *Cardozo Arts & Ent. LJ* 23 (2005), p. 1.

[7] Edward Lee. "The Ethics of Innovation: p2p Software Developers and Designing Substantial Noninfringing Uses Under the Sony Doctrine". eng. In: *Journal of Business Ethics* 62.2 (2005), pp. 147–162. ISSN: 0167-4544.

[8] Ugo Pagallo and Massimo Durante. "Three Roads to P2P Systems and Their Impact on Business Practices and Ethics". In: *Journal of Business Ethics* 90 (2009), pp. 551–564. ISSN: 01674544, 15730697. URL: http://www.jstor.org/stable/40863687.

[9] A. Mondal and M. Kitsuregawa. “Privacy, Security and Trust in P2P environments: A Perspective”. In: *17th International Workshop on Database and Expert Systems Applications (DEXA’06)*. 2006, pp. 682–686.

[10] Scott Wolchok and J Alex Halderman. “Crawling BitTorrent DHTs for Fun and Profit.” In: *WOOT*. 2010.

[11] Matthew Humphries. *French president Nicolas Sarkozy has broken his own three-strikes piracy rules*. Dec. 2011. URL: https://www.geek.com/news/french-president-nicolas-sarkozy-has-broken-his-one-three-strikes-piracy-rules-1450131/.

[12] Lee Mathews. *Your torrent download history is now available for everyone to see*. Dec. 2011. URL: https://www.geek.com/news/your-torrent-download-history-is-now-available-for-everyone-to-see-1448729/.

[13] *YouHaveDownloaded.com Alternatives*. Mar. 2018. URL: https://www.cogipas.com/youhavedownloaded-com-alternatives/.

[14] Anirban Banerjee, Michalis Faloutsos, and Laxmi Bhuyan. “The P2P war: Someone is monitoring your activities!” In: *International Conference on Research in Networking*. Springer. 2007, pp. 1096–1107.

[15] RIAA. *About Piracy*. 2020. URL: https://www.riaa.com/resources-learning/about-piracy/.

[16] Motion Picture Association. *Advancing Creativity*. 2020. URL: https://www.motionpictures.org/what-we-do/advancing-creativity/.

[17] 105th Congress. *Digital Millennium Copyright Act*. Oct. 1998. URL: https://www.govinfo.gov/content/pkg/PLAW-105publ304/pdf/PLAW-105publ304.pdf.

[18] Christopher Cotropia and James Gibson. "Higher Education and the DMCA". In: *Richmond Journal of Law and Technology* 25 (2 2018).

[19] 110th Congress. *Higher Education Opportunity Act*. Aug. 2008. URL: https://www.govinfo.gov/content/pkg/PLAW-110publ315/html/PLAW-110publ315.htm.

[20] South Texas College. *Digital Millennium Copyright Act*. URL: https://www.southtexascollege.edu/about/notices/dmca.html.

[21] UC Davis Office of Research. *The Digital Millennium Copyright Act (DMCA)*. URL: https://research.ucdavis.edu/industry/ia/researchers/copyright/dmca/.

[22] Carnegie Mellon University Information Security Office. *Digital Copyright and DMCA*. URL: https://www.cmu.edu/iso/aware/dmca/.

[23] David D'Amato. "Bittorrent Copyright Trolls: A Deficiency in the Federal Rules of Civil Procedure". In: *Rutgers Computer & Tech. LJ* 40 (2014), p. 190.

[24] Jacqui Cheng. *P2P leecher targeted in Germany for making files available*. July 2008. URL: https://arstechnica.com/tech-policy/2008/07/when-making-available-means-not-making-anything-available/.

[25] M. Comb and P. A. Watters. "Peeking behind the great firewall: Privacy on Chinese file sharing networks". In: *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. 2016, pp. 650–656.

[26] Neil Postman. "Five things we need to know about technological change". In: (1998).