Michał Czerniawski[1]

Graduated Response – a Comprehensive Solution in the War Against Online Piracy?

I. Introduction

The Safe Harbour doctrine,[2] which constitutes the current approach towards copyright infringement on the Internet, was created more than fifteen years ago in a totally different reality, where the Internet was considered as a new phenomenon and various governments wanted to stimulate development of the Web. In order to achieve this aim, governments decided to treat companies operating online commercially privileged. In the Safe Harbour system, Internet Service Providers (hereinafter: ISPs) are exempted from liability and allowed to forego taking any action against their subscribers until they become aware of subscribers' infringing activities, including copyright infringements. The role of ISPs is passive, mainly because there is no obligation for them to monitor what is happening within their networks. The two most influential pieces of legislation worldwide that include provisions establishing Safe Harbour system are the European Union's *E-Commerce Directive*[3] and the US *Digital Millennium Copyright Act*.[4]

Most of ISPs all around the world have adopted a passive approach toward copyright infringements, which has been difficult for copyright holders to accept. Moreover, at some point online piracy became a part of some online service providers' business model. There are many examples of companies misusing their limited responsibility arising out of the Safe Harbour, such as Rapidshare, or Chomikuj.pl.[5] In light of the foregoing, copyright holders in various

---

[1] Mgr prawa, doktorant na Wydziale Prawa Uniwersytetu Humanistycznospołecznego SWPS w Warszawie.

[2] Safe Harbour legal provisions protect Internet service providers from the consequences of their users' actions.

[3] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, Official Journal of the European Communities L 178/1.

[4] Digital Millennium Copyright Act (DMCA) of 1998, 17 U.S.C. § 512 (2006).

[5] List of copyright infringers based on the number of infringing URLs removed by

jurisdictions are seeking legislative changes and expect greater involvement from ISPs in copyright holders' fight against online piracy. One of the proposed solutions that may limit online piracy is so called "graduated response". Legal acts implementing graduated response were enacted in France, New Zealand, Taiwan, South Korea and the UK.[6] The most popular subtype of the graduated response is a "three strikes and you're out" approach, which allows the suspension or even termination of internet service provided to an infringer. An internet user allegedly infringing copyright laws receives two notices ("strikes"). The first one usually consists of information about copyrights, the second one is a legal warning and the third "strike" effects in suspension of subscriber's access to the Internet or other sanctions. The principle underlying a graduated response system is that sanctions should escalate as infractions increase.[7] Graduated response is being introduced also on contractual basis – the brightest example of such an approach is the voluntary Copyright Alert System (the so called six-strike" policy), introduced in 2013 in the United States as a result of a consensus reached between copyright holders and major American ISPs.[8]

Copyright holders definitely need a tool that will help them in protecting their interests.[9] However, when thinking about the graduated response one needs to bear in mind that the Internet is "not only an engine for free expression, it is a way to access culture and enhance education".[10] Moreover, access to the Web is already in some jurisdiction considered as a human right. For example, in Finland broadband internet access is a legal right for all citizens.[11]

Google as of September 2015, is available at Digital Music News: https://www.digitalmusicnews.com/2015/09/08/the-100-biggest-copyright-infringers-of-all-time-as-ranked-by-google/ (last visited: 28.03.2016).

[6] For detailed description of particular legal acts see R. Giblin, Evaluating Graduated Response, 37 Columbia Journal of Law & the Arts, pp. 147–209 (2014).

[7] A. Bridy, *Graduated Response and the Turn to Private Ordering In Online Copyright Enforcement*, "Oregon Law Review" 2010, Vol. 89, p. 128.

[8] For more details see M. Czerniawski, *How to protect users' personal data and enforce copyright on the Internet – Is there an alternative to cyber-surveillance?,* [in:] E. Schweighofer, F. Kummer, W. Hötzendorfer (eds.) Transparenz/Transparency, Tagungsband des 17. Internationalen Rechtsinformatik Symposions IRIS 2014, Österreichische Computer Gesellschaft, Vienna 2014, p. 551.

[9] Ibidem, p. 555.

[10] A. Strowel, *Internet Piracy as a Wake-up Call for Copyright Law Makers – Is the "Graduated Response" a Good Reply?*, WIPO J., no. 1(2009), p. 82.

[11] BBC, *Finland makes broadband a 'legal right'*, http://www.bbc.com/news/10461048 (last visited: 28.03.2016).

That is why, in my opinion, limitations on the right of Internet access should be imposed carefully, only under specific conditions.

II. Peer – to – Peer Networks

The most popular technology used for online copyright infringements is peer-to-peer. Therefore, before analyzing the issue of the graduated response it is important to explain what peer-to-peer networks are and how they have changed the Internet. A peer-to-peer (commonly abbreviated to P2P), is "any distributed network architecture composed of participants that make a portion of their resources (such as processing power, disk storage or network bandwidth) directly available to other network participants, without the need for central coordination instances (such as servers or stable hosts)".[12] Peers are both suppliers and consumers of resources. A real change came with the invention of the BitTorrent protocol. Beyond any doubt, the BitTorrent protocol is an example of "dual use technologies". These are products or services that can be used by the consumer in non-infringing ways, but can also be used to infringe copyright.[13]

The Swedish court in the well-known Pirate Bay case characterized BitTorrent technology as follows:[14]

> This technology means that files can be transferred between communicating computers which are on an equal footing with each other, i.e. neither has the role of client or host computer. There is no central computer in a network based on this technology. (...) BitTorrent software is used to divide a digital file into different segments and give them a mathematical number (known as a hash total), and to create a torrent file. A torrent file is a file which, in principle, contains only data which identifies the components the digital file has been divided into. To facilitate distribution of the digital file, an address for one or more trackers is, as a rule, specified in a torrent file.

---

[12] I looked at different definitions of peer-to-peer and found the Wikipedia one the most precise, https://en.wikipedia.org/wiki/Peer-to-peer (last visited: 28.03.2016).

[13] M.A. Lemley, R.A. Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, University of Texas Law and Economy Research Paper No. 025, p. 110.

[14] Verdict B 13301–06 handed down in Stockholm by the Stockholm District Court, Division 5, Unit 52, page 14 of translation made by the International Federation of the Phonographic Industry.

To sum up, P2P networks establish a direct connection between different Internet users, allowing them to share files without any kind of intermediary server and with very high transfer rate.

III. Safe Harbour Doctrine: the Notify and Take – Down Approach

As I have already mentioned, one of the factors that stimulate development of the Internet is the Safe Harbour doctrine, designed to limit ISP's liability for copyright infringements. A safe harbour constitutes *"[a]n area or means of protection [or a] provision (as in a statute or regulation) that affords protection from liability or penalty."*[15]

The Safe Harbour doctrine, by limiting their liability, allows ISPs to focus on their core business which is providing intermediary services (described below). As long as they follow some basic rules, ISPs do not have to worry about the risk of legal responsibility arising out of their customers actions, including for copyright infringements. In particular, they are not liable for copyrighted content they host as long as they have no knowledge in this respect. If they receive a proper notice of infringement they are obliged to take down the copyright infringing content.

The Safe Harbour doctrine was introduced for the first time in the *Digital Millennium Copyright Act* (hereinafter: *DMCA*) and soon became a global standard. Under the Safe Harbour doctrine the most fundamental condition of ISPs' immunity from liability is the lack of actual knowledge about the infringement taking place. De Beer and Clemmer studied Australia, Canada, China, the European Union, Japan, New Zealand, Singapore, South Korea and the United States and found that this requirement exists in the laws of each of these jurisdictions.[16]

Under the *E-Commerce Directive* there are the following ISPs' safe harbours: mere conduit, caching, and hosting. What distinguish the EU approach from the solution introduced in the United States is the fact that there is no information location tools safe harbour under EU law. Mere conduit is nothing but transmission of information. Under EU law ISPs are not liable for the information transmitted as long as they do not initiate the transmission,

[15] Black's Law Dictionary (8th ed. 2004).

[16] J. de Beer, Ch. D. Clemmer, *Global Trends in Online Copyright Enforcement: A No-Neutral Role for Network Intermediaries?*, 49 Jurimetrics J. (2009), p. 383.

do not select the receiver of the transmission and do not select or modify the information contained in the transmission.[17] Caching is an automatic, intermediate and temporary storage of information, performed for the sole purpose of making more efficient the information's onward transmission. In caching, ISPs are not liable for copyright infringements in particular when the catching does not modify the information.[18] ISP may not only transmit but also store information. Hosting is the storage of information. ISPs are not liable for hosting as long as they do not have knowledge of illegal activity or information and, upon obtaining such knowledge or awareness and act expeditiously to remove or to disable access to the information.[19] Article 15 of the directive states that Member States shall not impose a general obligation on providers, when providing mere conduit, caching and hosting to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

Under the DMCA there are four Safe Harbour exemptions: transitory communication, caching, hosting and information location tools. They are very similar to those implemented in the European Union. For example transitory communication mirrors the directive's mere conduit concept. The main difference between US and European law is the introduction of an information location tools safe harbour. Which means that although DMCA was enacted earlier than the directive, it includes one more exception than the EU law. In the US, an ISP may not be liable for the infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, such as a directory, index, reference, pointer, or hypertext link. To be on the safe side, the ISP cannot in particular have actual knowledge that the material or activity is illegal. Upon becoming aware of an infringement has to act expeditiously to remove, or disable access to, the material.[20]

It is important to note that the DMCA, similarly to the directive, in section 512(m) introduces provisions allowing ISPs not to monitor the content they transmit *via* their networks.

---

17 Article 12 of the Directive.

18 Article 13 of the Directive.

19 Article 14 of the Directive.

20 DMCA § 512 (d).

IV. Peer – to – Peer and Privacy

The question about the balance between copyright and privacy is not a new one. In 2003, Michael Geist, a law professor at the University of Ottawa, wrote:

> As privacy advocates began to react to the gradual deterioration of privacy protections in the name of security, they realized that it was necessary to promote a policy agenda that sought to protect both privacy and security. With a similar trend emerging in the intellectual property field, the privacy community must consider how it can promote a balanced approach that ensures respect for both intellectual property rights and personal privacy.[21]

Copyright holders in the United States did not have many problems with obtaining personal data of online copyright infringers. But outside the United States, courts often adopt a different point of view on the disclosure of personal information. The problem of establishing a fair balance between copyright enforcement and data protection is still unresolved. The most recognized European case regarding the personal data of copyright infringers is probably *Case C-275/06 Productores de Música de España (Promusicae) v Telefónica de España SAU* (Promusicae). In Canada the most significant case related to this issue is *BMG Canada Inc. v. John Doe*.[22] In both cases, the courts found the right to privacy of online pirates as a value that needs to be respected.

a) The C – 275/06 *Promusicae case*

The *Promusicae* case[23] originates in Spain. According to Promusicae in 2007 Spaniards spent €284 million on CDs and DVDs, compared to 367.3 million euros in 2006, which means that the industry noticed an €83 million decrease.[24] Although the industry admitted that sales accelerate in the digital market by 24%, the increase – according to Promusicae – was not enough to off-set

---

[21] M. Geist, *Web privacy vs. identifying infringers*, Toronto Star, Oct. 6, 2003. Available online at: http://www.michaelgeist.ca/resc/html_bkup/oct62003.html (last visited: 30.03.2016).

[22] 2005 FCA 193.

[23] Judgment of the Court (Grand Chamber) of 29 January 2008. Productores de Música de España (Promusicae) v Telefónica de España SAU (Case C-275/06).

[24] Information after International Federation of the Phonographic Industry: IFPI Research, document Music Market Data 2007.

toward the sale losses caused by piracy spread mostly by the P2P networks Kazaa[25] and eMule[26]. In the *Promusicae* a Spanish copyright collective demanded disclosure of personal data of Kazaa users from Telefónica, the biggest Spanish ISP. The European Court of Justice ruled that:

> (...) the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.[27]

The European Court of Justice held that, under the EU law, Member States are not obliged to implement laws that would force ISPs to disclose their subscribers' data for the purpose of copyright infringement claims raised in civil proceedings. However, if any of the Member States does so, it should secure a fair balance between the right to property and right to privacy, two fundamental rights protected by the EU legal order, in particular by the Charter of the Fundamental Rights of the European Union. The verdict maintained a *status quo* and shall be considered as shifting this duty to balance the above mentioned rights to the Member States and national courts.

The debate within the European Union whether an IP address is personal data was ended by the Article 29 Data Protection Working Party (hereinafter: "Working Party"), an advisory body to the European Commission which brings together representative of European data protection authorities. In the Opinion 4/2007[28] the Working Party stated that:

> (...) especially in those cases where the processing of IP addresses is carried out with the purpose of identifying the users of the computer (for instance, by Copyright holders in order to prosecute computer users for violation of intellectual property rights), the controller anticipates that the 'means likely reasonably to be used' to identify the persons will be available e.g. through

[25] Kazaa Media Desktop was a very popular peer-to-peer file sharing application.

[26] eMule used to be a very popular peer-to-peer file sharing application.

[27] Promusicae, at 71.

[28] Opinion 4/2007 on the concept of personal data, adopted on June 20, 2007, 01248/07/EN, WP 136.

the courts appealed to (otherwise the collection of the information makes no sense), and therefore the information should be considered as personal data.

According to Peter Hustinx, the former European Data Protection Supervisor, IP addresses and the information about the activities linked to such addresses constitute personal data in all cases relevant to graduated response.[29] Also dynamic IP addresses shall be considered as personal data.[30]

b) John Doe v. BMG

The issue of establishing balance between copyright enforcement and privacy was also the subject of judicial proceedings in Canada. In *BMG Canada Inc. v. John Doe*,[31] the plaintiffs, seventeen music recording companies, members of the Canadian Recording Industry Association (CRIA), demanded information from five Canadian ISPs regarding the users of 29 IP addresses, suspected of illegal download of copyrighted music files *via* P2P networks. The 29 defendants were identified only by their P2P pseudonyms and IP addresses. Citing privacy concerns,[32] the ISPs refused to provide the names of the Internet users without a court order.

On March 31, 2010, the judgment of the Federal Court of Canada was delivered. The court held that in order to divulge personal information of ISPs' subscribers the following criterions must be met: a) the applicant must establish a *prima facie* case against the unknown alleged wrongdoer; b) the person from whom discovery is sought must be in some way involved in the matter under dispute, he must be more than an innocent bystander; c) the person from whom discovery is sought must be the only practical source of informa-

[29] Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA) – 2010/C 147/01 adopted on 22 February 2010, at 27 and Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America – 2012/C 215/08 adopted on 24 April 2012, at 19.

[30] Judgment of the Court (Second Chamber) of 19 October 2016 (request for a preliminary ruling from the Bundesgerichtshof – Germany) – Patrick Breyer v Bundesrepublik Deutschland (Case C-582/14)

[31] *BMG Canada Inc. v. John Doe*, 2004 FC 488 aff'd 2005 FCA 193.

[32] Canada has a specific law relating to personal data protection called *Personal Information Protection and Electronic Documents Act* (abbreviated PIPEDA), S.C. 2000, c. 5.

tion available to the applicants; d) the person from whom discovery is sought must be reasonably compensated for his expenses arising out of compliance with of the discovery order in addition to his legal costs; e) the public interests in favour of disclosure must outweigh the legitimate privacy concerns.[33]

The test developed by the judge in *BMG Canada Inc. v. John Doe* was modified in the Canadian Federal Court of Appeal decision. The court stated that in order to divulge personal information of ISPs' subscribers following criterions must be met:

a) The applicant must show that it has a *bona fide* (made in good faith) claim against the proposed defendant, *"(...) i.e. that they really do intend to bring an action for infringement of copyright based upon the information they obtain, and that there is no other improper purpose for seeking the identity of these persons."*[34]
b) The claim must be based on evidence linking the pseudonyms/IP addresses with the impugned actions.[35]
c) The plaintiff has to prove that the information cannot be obtained from another source (such as the operators of the websites). Also "*if an order for disclosure were granted, consideration would have to be given to the costs incurred by the respondents in assembling the information*".[36]
d) "*[T]he public interest in favour of disclosure must outweigh the legitimate privacy concerns of the person sought to be identified if a disclosure order is made.*"[37]
e) "*[T]he greatest care should be taken to avoid delay between the investigation and the request for information. Failure to take such care might well justify a court in refusing to make a disclosure order.*"[38]
f) "*[P]laintiffs should be careful not to extract private information unrelated to copyright infringement, in their investigation*"[39]

In this proceeding Sexton J.A., one of the appeal judges stated that "[t] his case illustrates the tension existing between the privacy rights of those

[33] FC 488, at 13.
[34] 2005 FCA 193, at 34.
[35] 2005 FCA 193, at 21.
[36] 2005 FCA 193, at 35.
[37] 2005 FCA 193, at 36.
[38] 2005 FCA 193, at 43.
[39] 2005 FCA 193, at 44.

who use the Internet and those whose rights may be infringed or abused by anonymous Internet users".[40] As the criterion mentioned above were not met, in this case the court stated that under Canadian law the identities of ISPs' subscribers should not be revealed to the CRIA.

Deprived of a possibility to obtain personal data of online copyright infringers under legislation being in force at that time, copyright holders all around the world, began to seek different solutions, the graduated response system being one of them.

V. Controversies Around the Graduated Response

The aim of the graduated response system is to protect the interests of copyright holders and provide sufficient warning to online copyright infringers. There are three factors needed for graduated response to function: a) monitoring of users' online behavior; b) capture of users' IP addresses and matching of a captured address to a particular ISP's subscriber's account; c) collection of users' data.[41] Usually, warnings are being escalated and culminate in the termination of the subscriber's Internet connection. This solution is controversial as access to the Internet became in many countries an essential part of daily life.

To certain extend this approach seems to be justified. Yu is right stating that respect for the copyright system has drastically gotten eroded since the emergence of Napster, the first file-sharing software.[42] People all around the world got used to things such as "free" music files and videos on the Internet. This is one of the reasons why copyright holders proposed a radical solution such as the graduated response. It also means that the key to the victory in a fight with web based copyright infringement might lie in changing the behavior of internet users, in particular those who upload illegal content.

Many people understand the graduated response system as something that always leads to the termination of an Internet account and that the termination is the only sanction used in these systems. They are, for the most part, wrong. There is a whole range of possible third "strikes" – sanctions aimed at solving the problem of repeated infringements, such as slowing down the speed of Internet connection, or blocking specific web pages. Termination of the access to Internet is a sanction that is used in the most extreme circumstances, practice

---

40 *BMG Canada Inc. v. John Doe*, 2005 FCA 193 at 2.

41 M. Czerniawski, op.cit., p. 551.

42 P.K. Yu, *The Graduated Response*, Florida Law Review, Vol. 62, 2010.

showed that it is imposed extremely seldom.[43] Below I will describe different approaches towards the graduated response system.

a) Effectives

One of the biggest controversies surrounding the graduated response is the issue of its effectiveness. This approach was designed to fight copyright infringements which take place *via* peer-to-peer networks. However, Internet users, aware of how the graduated response works, may keep infringing copyright through other means of obtaining copyrighted content in the Internet – in particular illegal streaming sites and HTTP-based download services.

On the other hand, some scholars state that the real effect of law introducing the graduated response is an influence it has on "average" people. The graduated response is seen as a deterrent to copyright infringing behaviour. Even the term *three strikes and you are out* is aimed at deterring people. The graduated response can work as a deterrent, but only in some cases – for example parents of young online copyright infringers, after receiving the first notice, may immediately forbid their children sharing illegal content. Therefore, the solution ineffective from a legal/enforcement point of view may appear to be very efficient from psychological perspective, convincing people not to get involved in online copyright infringements. At the same time, persistent copyright infringers, in particular those with some technological knowledge, may be always able to find a way to share illegal content with legal impunity.

b) Freedom of Expression

Society we live in is considered an information society. Beyond any doubt, the main source of any kind of information is the web. The Internet is a way to access information, culture, enhance education. The Web is not only a key tool for exercising freedom of expression (for example, *via* blogs or comments posted online) but also an extremely important instrument allowing people to communicate with each other. The Internet has become an inseparable part of modern life. There is a large number of businesses based solely online, moreover for instance, many online shops offer better prices than their stationary counterparts. Many schools, including universities, offer e-learning courses. This circumstance may have a significant meaning for some groups of people, such as disabled individuals or other persons not able to leave place where

[43] For a detailed analysis see R. Giblin, op.cit., pp. 157–180.

they live in order to attend classes. The Internet is also a source of innumerable opportunities. The Web is being used by all kind of artists as an instrument for promotion of their art, by businessmen for developing their business activities, by journalists presenting their opinion and by politicians for public debate. Almost all social groups benefit from access to the Web. With websites helping to find a job, giving advice or being a source of all kind of knowledge about contemporary world, a suspension of access to the web might be seen even as discrimination and may have serious economic consequences to an individual.

c) Costs

A very important issue connected with the implementation of a graduated response system are costs. Legislations such as the French HADOPI law[44] or the New Zealand act,[45] establish new institutions aimed at dealing with copyright infringers. New bureaucracy always means new expenses. But the main costs connected with implementation of a graduated response system are the costs of the monitoring of the ISPs' networks. This is one of the reasons why some ISPs were against introduction of the graduated response. The costs for ISPs are high because in most cases, under the graduated response system, ISPs are required to:

- identify the IP address and match it to the account holder;
- retain data on infringements;
- provide right holders with information about repeat infringement;
- be able to determine when a repeat copyright infringement has occurred;
- forward notices to account holders and counter-notices to copyright holders;
- communicate with right holders.

All those tasks are new to ISPs and require development of a proper infrastructure.

According to the *Digital Economy Act Impact Assessment*[46] the cost of introduction the graduated response in the UK where supposed to be between £290–500 million.[47] The assessment identifies following groups of costs:

---

[44] French Loi n°2009–669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, JORF n°0135 du 13 juin 2009 p. 9666.

[45] Copyright (Infringing File Sharing) Amendment Act, 2011.

[46] *Digital Economy Act Impact Assessment.* Available online at: http://webarchive.nationalarchives.gov.uk/20100511084737/http:/interactive.bis.gov.uk/digitalbritain/wp-content/uploads/2010/04/Digital-Economy-Act-IAs-final.pdf (last visited: 30.03.2016).

[47] Op.cit., p. 17.

> Costs to ISPs of complying with the legislation, including costs of notifying infringers, capital costs to ISPs, costs of setting up and running a call centre, annual capital and operating costs to mobile network operators. Possibility of higher broadband costs for consumers.(...) Costs to low income/low valuation digital product consumers who would stop consuming digital content altogether rather than purchase it; costs to rights holders of identifying infringing IP addresses and taking infringers to court.[48]

d) Accuracy of the Infringement – identifying Technology (False Positives)

Another important issue that arises when we talk about the graduated response, is accuracy of the infringement-identifying technology. Yu mentions a number of mistakes made by copyright holders (mainly by the American RIAA) at the time they were suing people uploading or downloading copyrighted content *via* P2P networks:

> (...) the industry's web-crawlers confused an a cappella song about a gamma ray satellite developed by Pennsylvania State University with the highly-downloaded songs of a best-selling rhythm-and-blues artist. (...) Warner Brothers misidentified a child's book report on Harry Potter and the Sorcerer's Stone as an infringing Harry Potter movie, even though the file is in .rtf format. A 66-year-old Boston woman was accused of offering hardcore rap songs, like 'I'm a Thug', for download, even though her computer was incapable of running the file-swapping software she allegedly had used (...) And the most troubling of all, a lawsuit was filed against an 83-year-old deceased woman who hated computers during her lifetime, causing one newspaper reporter to write: "death is no obstacle to feeling the long arm of the Recording Industry Ass. of America".[49]

Infringement-identifying technology is constantly being improved. However, it is not possible to totally eliminate false positives, thus – there will always be a number of cases where legal actions would be initiated against Internet users qualified as copyright infringers by mistake.

---

[48] Ibidem.

[49] P.K. Yu, op.cit., pp. 15–16.

e) Privacy and the Issue of Deep Packet Inspection

The graduated response is also an issue of content filters. Under some legislations, such as HADOPI law, a subscriber may be forced to install special filters. The filters are usually based on a technology called Deep Packet Inspection (DPI). Lessig described the role of ISPs in the Internet using the example of daydreaming postal worker, who only moves the data and leaves interpretation of the data to the applications at either end.[50] Bendrath, basing on Lessig's postal worker example, describes DPI technology as follows:

Imagine a postal worker who is not just daydreaming and moving packets from one point to another in the transportation chain. Imagine the postal worker

- opens up all packets and letters,
- inspects and even reads the content,
- checks it against databases of illegal material and if finding a match, sends a copy to the police authorities,
- destroys letters he finds having prohibited or immoral content,
- sends packets with content from those mail-order companies which pay extra to the postal service to a special and very fast delivery truck, while the ones from the competitors go to an extra-slow and cheap sub-contractor.[51]

Nowadays, all this monitoring may happen without significant delays and damages to the data that is being sent. Frieden stated that "*ISPs probably will collaborate with copyright holders perhaps going so far as to program hardware with deep packet inspection software that achieve both traffic management goals, to pursue price and QOS [quality of service] diversification, as well as DRM [Digital Rights Management], to mollify the copyright holders.*"[52] This issue raises of course privacy concerns. Bridy states that, for example, in the United States:

---

[50] L. Lessig, *Code 2.0.*, New York 2006, p. 44.

[51] R. Bendrath, *Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection,* available online at: *http://userpage.fu-berlin.de/~bendrath/Paper_Ralf-Bendrath_DPI_v1–5.pdf* (last visited: 30.03.2016).

[52] R. Frieden, *Internet Packet Sniffing and its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers*, p. 45. Available online at SSRN.

> 'there is a compelling legal reason for ISPs to consider the prospect [DPI] seriously. As broadband providers have abandoned the end-to-end model of data transit in favor of intrusive traffic management or shaping, their continuing eligibility for the – mere conduit safe harbor in section 512(a) has become questionable. To the extent that their network management practices now entail active intervention at the level of content, ISPs have exposed themselves to copyright liability from which section 512(a) shielded them when they were content to be – dumb pipes.'[53]

f) The Issue of IP Addresses

There is one more graduated response issue worth mentioning. It is relatively easy for an Internet user to conceal his/her identity by using so called "IP spoofing". IP spoofing is a "*creation of Internet Protocol (IP) packets with a forged source IP address, (...) with the purpose of concealing the identity of the sender or impersonating another computing system.*"[54] It looks that concealing own identity through technological means is one of the easiest methods that might guarantee online copyright infringers' impunity.

In many public places, such as the shopping malls, coffee shops, airports, libraries or fast-foods so called hot spots, free Wi-Fi access points are available. Legislators try to solve the issue of copyright infringement done via public networks. As the recent CJEU C-484/14 *McFadden* case shown, this issue still remains unresolved. In *McFadden* copyright-protected content passed through a German citizen's unprotected, freely-accessible Internet connection, and was made available to Internet users *via* a file-sharing site. The question arises, whether in such a situation owner of the Wi-Fi access point may be held liable for copyright infringement.

Another issue is that many users, especially older people, are not familiar with wi-fi modems and do not know how to effectively protect their local networks. Even after receiving notices from copyright holders they might not be able to find out that someone is using their Internet connection. What to do in such case? Should people be punished just because they are not familiar enough with new technologies?

---

[53] A. Bridy, *Graduated Response and the Turn to Private Ordering*, Oregon Law Review, Vol. 89, 2010, p. 106.

[54] After Wikipedia: http://en.wikipedia.org/wiki/IP_address_spoofing (last visited: 30.03.2016).

g) The Issues of Copyright Exceptions

Exceptions and limitations are present in all copyright systems around the world. The implementation of the graduated response will make exercising of institutions such as fair use or fair dealing much more complicated and may lead to many disputes between ISPs' subscribers and copyright holders. A good example here is the Digital Right Management (DRM) technology. In 2004 Ian Kerr stated that "*[t]he technologies employed by DRMs are not yet sufficiently sophisticated to mirror the law of copyright because TPMs themselves remain incapable of distinguishing between infringing and non infringing uses of digital works.*"[55] In 2017, DRM technologies still are not able to recognize and apply copyright exceptions. Currently, algorithms are not able to recognize that, for example, music in the video on YouTube was used for parody purposes which is a copyright exception under the DMCA and does not constitute a violation of copyrights.

h) The Issue of Alternatives to P2P

All the versions of the graduated response are aimed at addressing infringement in P2P networks. Although P2P protocol is currently the biggest source of an online copyright infringement, there are also other sources of online piracy such as HTML based download or illegal streaming. Internet pirates may easily adapt to a new reality created by the graduated response, and switch to alternative methods of sharing illegal content.

One of the consequences of implementing the graduated response all around the world might be that P2P users will simply switch to alternative sources of copyrighted content such as illegal streaming sites and HTTP-based download services, which are not covered under the graduated response legislation. Copyright holders have already noticed this issue. They began to put pressure on HTTP-based download services, in particular on the biggest one – RapidShare. For example, on May 3, 2010, in a case brought by movie distributor the Capelight Pictures against RapidShare, the Düsseldorf higher regional court judged that RapidShare could not be held liable for copyright infringements by its users.[56] On February 10, 2010 a German court in Hamburg

[55] I. Kerr, *Technological Protection Measures: Part II – The Legal Protection of TPMs*, Department of Canadian Heritage, Copyright Policy Branch, Online, December 15, 2004.

[56] The verdict no. I-20 U 166/09 is available online (in German) at: http://www.tele-

handed down a judgement, in which the court ordered RapidShare to implement measures (in this case proactive book titles filtering) to prevent illegal file sharing of the 148 copyright-protected works from six global publishers. [57] The court ruled that the company is obliged to monitor its website in order to ensure the copyrighted material is not being uploaded. Moreover, under the ruling RapidShare has to prevent unauthorized access to the copyrighted material by its users.

i) Lack of Availability of Copyrighted Content via Legitimate Channels

The problem may lay also in lack of legal sources of particular content. For example, Netflix, global provider of streaming movies and TV series, still does not operate on many markets. Only recently, this very popular streaming platform, became available in Poland. In the past it was not possible to obtain content offered by Netflix without infringing copyrights.

VI. Alternatives of the Graduated Response

1. The Notice – and – Notice Approach

The notice-and-notice approach is a Canadian solution aimed at fighting online copyright infringements, created after the verdict in the *BMG Canada Inc. v. John Doe* case. It was introduced in Canada in the Copyright Modernization Act.[58] Michael Geist described the mechanism of the notice-and-notice approach as follows:

> 'The notice and notice system involves a notification from a copyright holder – often involving movies, software or music – claiming that a subscriber has made available or downloaded content without authorization on file sharing systems. The Internet Service Provider forwards the notification

medicus.info/urteile/Internetrecht/Haftung-von-Webhostern/1017-OLG-Duesseldorf-Az-I-20-U-16609-Keine-Haftung-von-Rapidshare-fuer-Urheberrechtsverletzungen-Dritter.html (last visited: 30.03.2016).

[57] See: *Global Publishers Win Ruling to Stop Rapidshare from Profiting from Pirated Works*. Press release available online at: http://eu.wiley.com/WileyCDA/PressRelease/pressReleaseId-69777.html (last visited: 30.03.2016).

[58] C-11, 41st Parliament, 1st Session.

> to the subscriber but takes no other action – it does not pass along the subscriber's personal information, remove the content from its system, or cancel the subscriber's service.'[59]

The main weakness of this system is that the effectiveness of the notice-and-notice approach is mainly based on a belief that subscribers will stop downloading illegal content after they receive a notification from copyright holders. This conviction is based *inter alia* on the survey in which 70% of Internet users declared to cease downloading of copyrighted content after receiving first notice. It is hard to imagine that persistent "pirates", aware that the notice will not be followed by any kind of sanctions, will stop copyright infringing activities. But this is the weakness of all solutions proposed by copyright holders, including the graduated response. However, it seems that most of the copyright infringers are "occasional" pirates.

The great advantage of the notice-and-notice solution is that it is subscriber-friendly and works with minimal customer complaints. It also helps in educating subscribers about copyright in the Internet, raising their awareness about online piracy and its legal consequences. In some cases it might also work as a deterrent – as in, mentioned already, case of parents of young online copyright infringers, who after receiving the first notice, will immediately forbid their children sharing illegal content.

As for now, the notice-and-notice approach was formalized only in Canada. The new law entered into force on 2nd January 2015, that is why it is still too early to say how effective it is. I will not be surprised if it appears that there is no difference between the effectiveness of the graduated response and the notice-and-notice. In such cases the notice-and-notice approach, as the less inconvenient for ISP subscribers, seems to be the best option. Persistent copyright infringers, in particular those with some technological knowledge, will be always able to find a way how to share illegal content with legal impunity. But legislators design systems aimed at addressing concerns for the majority of users not for the minority that is very tough to stop. Notice-and-notice approach should successfully address concerns for "casual" copyright infringers, which are the significant majority of all online pirates.

---

[59] M. Geist, *The Effectiveness of Notice and Notice,* after: http://www.michaelgeist.ca/content/view/1705/125/ (last visited: 30.06.2016).

2. The Notice – and – Slowdown Approach

It seems that a good alternative to the graduated response system might be the notice-and-slowdown approach. This solution can be applied simultaneously with the graduated response or with the notice-and-notice solution. For example, under the British Digital Economy Act[60] possible technical measures include limiting the speed or other capacity of the service provided to a subscriber. HADOPI law seems to support filtering as it states that an online copyright infringer might be forced to take appropriate security measures.

ISPs in the past were already throttling internet traffic. For example in 2007, Comcast, an American ISP, used a DPI technology to throttle BitTorrent traffic. In 2008, it was sanctioned for this conduct by the U.S. Federal Communications Commission. However, in 2010, the United States Court of Appeals for the District of Columbia Circuit ruled that the commission did not have the authority to force Comcast not to stop slowing P2P traffic.[61]

The notice-and-slowdown approach allows ISP subscribers to stay connected to the Web and simultaneously makes P2P file sharing impossible. That is why it appears to be a solution worth considering when fighting online piracy.

3. The Notice-and-Slowdown Approach – Controversies

Nevertheless, the notice-and-slowdown system is not a perfect solution. It has the same weaknesses as the graduated response with exception of the most important one – the notice-and-slowdown approach respects the fundamental right to the freedom of expression. A copyright infringer still benefits from the access to the Web, but downloading of large amounts of data is an extremely inconvenient and time consuming task.

The notice-and-slowdown approach would be, as in the graduated response case, a very unpopular solution. According to Bridy during, mentioned above,

---

[60] Under section 124G of the Digital Economy Act, the Secretary of State can request OFCOM, an independent regulator and competition authority for the British communications industries, to assess whether technical obligations should be imposed on ISPs. A technical obligation is an obligation to take technical measures against a subscriber that infringes copyright which include suspension of the service provided to a subscriber.

[61] C. Kang, *Court rules for Comcast over FCC in 'net neutrality' case*, The Washington Post, April 7, 2010. Available online at: http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040600742.html (last visited: 30.03.2016).

Comcast torrent throttling episode, "*the ISPs responsible for most of the [BitTorrent upload] blocking had not publicly disclosed their network management practices*."[62] It seems that Comcast did not want to inform its customers about how its networks are being managed as it was afraid of their potential reaction. Connection speed is one of the main reasons for ISP customers' complaints.

One of the controversial forms of throttling of the Internet connections is a blockade of P2P protocol in ISP network. The controversies arise because P2P protocols are being used also for non-infringing purposes, such as VoD (Video on Demand) and other data transfers such as game download.[63] Implementation of the P2P protocol blockade would force many companies to look for alternative solutions such as download based on HTML. As more and more sophisticated software is being created some of the problems connected with connection throttling might be overcome. For example, Comcast, after resigning from P2P protocol blockade, implemented a solution in which possible connection throttling affects only selected traffic and does not affect real-time protocols like VoIP and gaming.[64]

Another issue connected with the throttling are technological capabilities of ISPs' networks. Under the graduated response an ISP is obliged to block a particular IP address – this action is relatively easy to take as it is possible to precisely indicate which IP address should be disconnected. Under the notice-and-slowdown approach an ISP has to throttle a particular Internet connection without slowing down other subscribers. Such precise action might be technologically impossible to take in some networks – as many people might share the same connection, throttling one of them will affect other subscribers. Reisman explains that "a typical provider starts out with a big pipe of Internet access that is shared via exchange points with other large providers. They then subdivide this access out to their customers in ever smaller chunks — perhaps starting with a gigabit exchange point and then narrowing down to a 10 megabit local pipe that is shared with customers across a subdivision or area of

---

62 A. Bridy, op.cit. p. 130.

63 See for example S. Annapureddy, Ch. Gkantsidis, P. Rodriguez, L. Massoulie, *Providing Video-on-Demand using Peer-to-Peer Networks*, available online at: http://www.scs.stanford.edu/~reddy/research/redcarpet/redcarpet.pdf (last visited: 30.03.2016).

64 After: N. Anderson, E. Bangeman, *Comcast loses P2P religion, goes agnostic on throttling*, Ars Technica, September 19, 2008. Available online at: http://arstechnica.com/old/content/2008/09/comcast-loses-p2p-religion-goes-agnostic-on-throttling.ars (last visited: 30.03.2016).

town."[65] Usually subscribers from the same area share the same Internet pipe making precise throttling difficult or even impossible for an ISP.

VII. Conclusion

Copyright holders definitely need a tool that will help in protecting their interests. However, the graduated response might end up as a system which fails to meet the hopes placed in it. Although different countries propose different approaches towards the graduated response the main controversies all common to all the systems. The main arguments against the graduated response system are its costs, questionable effectiveness and issue of freedom of expression. The graduated response system is also not flexible and address only one source of online piracy – P2P networks. Moreover, as I argue, the graduated response will force only "occasional" copyright infringers to stop unlawful downloading. Persistent copyright infringers, in particular those with some technological knowledge, will always be able to find a way to share illegal content with legal impunity. That is why an alternative solutions such as the notice-and-notice and notice-and-slowdown shall be able to successfully replace the graduated response and achieve similar results in fighting online piracy without violating the freedom of expression. On the other hand, thanks to the graduates response, to certain extent copyright holders already achieved one of their goals – people all around the world became more aware of the consequences of a copyright infringement in the Web.

Is a graduated response system a balanced solution, protecting not only copyright but also human freedoms, in particular freedom to receive information and privacy? In my opinion it is not the case if the legal instrument may, even potentially, deprive ISP subscribers of a key instrument in the information society – access to the Web. I, therefore, see two alternatives to graduated response: notice-and-slowdown and notice-and-notice approaches. Sanctions introduced in these systems, such as Internet throttling or in case the throttling is technically impossible – warning screen – are not drastic but inconvenient for ISP subscribers and in most cases should be enough to make copyright infringers stop downloading and uploading illegal content. In many situation a single notification, a clear indicator that particular user was identified as a copyright infringer, may be sufficient to limit violations. In any case, legislators around the world should realize that intellectual property has to be protected in the way that respects subscribers'

[65] A. Reisman, *Analysis: The White Lies ISPs Tell About Broadband Speeds*, Netequalizer, March 21, 2009. Available online at: http://netequalizernews.com/2009/03/21/analysis-the-white-lies-isps-tell-about-broadband-speeds/ (last visited: 30.03.2016).

rights and freedoms. Moreover, legal instruments shall be always accompanied by other means, in particular education of Internet users in the field of copyright law.

Summary

Escalation of online copyright infringements resulted in a worldwide shift in laws aimed at fighting illegal file sharing on the Internet. A new model of cooperation between copyright holders and Internet Service Providers was created. This cooperation is called the graduated response. In its most restrictive version this system allows suspension or even termination of the Internet service provided to the ISP's subscriber who infringed copyrights.

Copyright holders definitely need a tool that will help in protecting their interests. In this paper I analyze graduated response system in order to demonstrate its advantages and weaknesses. I conclude that legislators around the world should consider alternative solutions to the issue of online piracy such as the notice-and-slowdown and the notice-and-notice approach. I prove that intellectual property might and should be protected online in an effective manner which respects subscribers' rights and freedoms, in particular the right to access to the Internet.

Keywords: Copyright law, Copyright Law Protection, Internet Services

Streszczenie

Nasilenie się zjawiska naruszeń praw autorskich w Internecie przyczyniło się do powstania całkowicie nowych rozwiązań mających na celu walkę z nielegalną wymianą treści online. Powstał nowy model współpracy podmiotów uprawnionych z tytułu praw autorskich z dostawcami usług internetowych – tzw. graduated response. W jego najbardziej restrykcyjnej wersji dopuszcza on zawieszenie albo odcięcie usługi dostępu do Internetu naruszycielowi.

Bezsprzecznie, podmiotom uprawnionym z tytułu praw autorskich potrzebne są narzędzia ochrony tych praw. W niniejszym artykule analizuję koncepcję graduated response wskazując jej zalety i wady oraz stwierdzając że warte rozwagi są rozwiązania alternatywne: notyfikacja-i-spowolnienie (notice-and-slowdown) oraz notyfikacja-i-notyfikacja (notice-and-notice). Poza wszelką wątpliwością własność intelektualna powinna być chroniona w Internecie. Powinno to się odbywać w sposób efektywny i jednocześnie z poszanowaniem praw i wolności usługobiorców, w szczególności ich prawa dostępu do Internetu.

Słowa kluczowe: Prawo autorskie, ochrona praw autorskich, usługi internetowe