

NOVEL REMEDIES FOR INTELLECTUAL PROPERTY RIGHTS INFRINGEMENT ONLINE

Mindaugas Kiškis

Institute of Digital Content
Faculty of Social Technologies
Mykolas Romeris University
Ateities st. 20, LT-08303 Vilnius, Lithuania
Telephone: (+370 5) 271 4711
E-mail: mkiskis@mruni.eu

Received on 11 September 2013; accepted on 28 December 2013.

doi:10.13165/JUR-13-20-4-09

Introduction

The last decade along with the explosion of the broadband Internet and peer-to-peer (P2P) technologies transformed the Internet into primary vehicle for infringement of intellectual property rights (IPR), as well as many other illicit activities. This has been recognized internationally through unification of the substantive legal rules governing illicit online activities in the Council of Europe Cybercrime Convention 2001 and other documents, as well as more recently by addressing the issues of enforcement online in the EU Enforcement Directive 2004/48/EC and the Anti-Counterfeiting Trade Agreement. Despite these initiatives, existing legal remedies available to the IPR holders, including the newest initiatives on the “three strike” approach to infringing Internet subscribers, as well as filtering/blocking of illicit Internet resources, are frequently referred to as insufficient and ineffective. Empirically, they failed to contain the rise of digital piracy in any meaningful way, thus, highlighting the need for novel remedies against intellectual property infringements online.

In the paper, the main problem of the failure of existing “offline” remedies, as well as newer “three strikes” and Internet filtering remedies, to tackle copyright and related rights infringement on the Internet are analysed. The purpose of the paper is to argue a case for the novel online remedy, focused on domain seizure. Principal socio-legal reasons for such failures are reviewed and analyzed, key features of the efficient online remedies are identified. The paper also looks at successful cases of enforcing rights online. Domain seizure/takeover through the existing Uniform Domain Name Dispute Resolution Policy (UDRP) system is reviewed as a successful online instrument dealing with trademark rights infringement online. The author considers expansion of the domain seizure remedy judicially and through UDRP to cover most pervasive copyright and related rights infringements as a viable alternative (addition) to the existing remedies for the rights holders to deal with such infringements online.

The topic of the paper has not been exhausted in previous legal research. In Lithuania, only the general remedies for copyright and related rights¹ and specific of the intellectual property infringements online² have been analyzed. Abroad, the analysis has been focused mainly on the specifics of the violations for different types of intellectual property rights. Most researchers have focused on the promotion or criticism of the three-strikes and Internet filtering/blocking as solutions for online infringements. Non-elaborate ideas that completely new remedies are needed have only been suggested by the US legal scholars³. Content analysis, as well as comparative, teleological, phenomenological and epistemic analysis methods are employed for the research presented in the paper.

1. Recent legal initiatives on remedies for infringement of intellectual property rights online

Since the EU Enforcement Directive 2004/48/EC, the most active attempts to adopt new remedies against infringement of intellectual property laws online have been made at national level. One prominent national initiative focuses on the “three strikes” (recently renamed – graduated response) approach, implemented in France and other countries⁴. The European Data Protection Supervisor has precisely summarized the approach as follows: “*copyright holders using automated technical means, possibly provided by third parties, would identify alleged copyright infringement by engaging in monitoring of Internet users’ activities, for example, via the surveillance of forums,*

-
- 1 Mizaras, V. Intelektinės nuosavybės teisių gynimo reglamentavimo novelos Europos Bendrijos teisėje: pagrindiniai principai. *Teisė*. 2005, 55: 95–118.
 - 2 Kiškis, M.; Petrauskas, R. Intelektinės nuosavybės elektroninėje erdvėje pažeidimų ypatumai. *Jurisprudencija*. 2006, 5(83): 29–36.
 - 3 Lemley, M. A.; Reese, R. A. Reducing Digital Copyright Infringement without Restricting Innovation. *Stanford Law Review*. 2004, 56(1345) [interactive]. [accessed on 15-06-2013]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=525662>.
 - 4 Brown, I. Internet Self-Regulation and Fundamental Rights. *Index on Censorship*. 2010, 1(39): 98–106 [interactive]. [accessed on 15-06-2013]. <<http://ssrn.com/abstract=1539942>>.

blogs or by posing as file sharers in peer-to-peer networks to identify file sharers who allegedly exchange copyright material. After identifying Internet users alleged to be engaged in copyright violation by collecting their Internet Protocol addresses (IP addresses), copyright holders would send the IP addresses of those users to the relevant Internet service provider(s) who would warn the subscriber to whom the IP address belongs about his potential engagement in copyright infringement. Being warned by the internet service provider (ISP) a certain number of times would automatically result in the ISP's termination or suspension of the subscriber's Internet connection."⁵ These initiatives have lately gained spotlight in the context of the Anti-Counterfeiting Trade Agreement (ACTA) provisions requiring the ISP's involvement in identifying the infringing subscribers. The ACTA attempted to formalize new obligations (remedies) against online service providers, which, according to Article 27 Paragraph 4 of the ACTA, may be ordered to disclose information on a subscriber, whose account was used for infringement, thus, enabling legal action against such subscribers. Concerns that such provisions may not be in line with the fundamental rights⁶ have led to the demise of the ACTA in the EU.

Another effort aimed at remedying IPR infringements online focuses on blocking or filtering of certain Internet resources, which contain unauthorized content or facilitate access to such content. Blocking or filtering has been attempted based on Internet protocol (IP) address and domain name system (DNS) filtering, i.e., filtering all Internet resources available under a specific IP address or domain name. More recently, Deep Packet Inspection (DPI) filtering approach has been considered, which involves live screening of the packets of information, which are being transmitted and received by the network hosts. Studies on the effects of such filtering⁷ found them controversial in their efficiency and having potential to infringe fundamental rights, which led the affected parties to the Court of Justice of the European Union (CJEU), which recently ruled on two cases pertaining to Internet filtering for dealing with copyright infringements.

The CJEU decision in the *Scarlet Extended* case C-70/10 formulated five criteria for when filtering is not deemed legally proportional:

1. when filtering affects all electronic communications passing via its services, in particular those involving the use of peer-to-peer software;
2. filtering, which applies indiscriminately to all its customers;
3. filtering as a preventive measure;
4. filtering, exclusively at ISP expense; and

5 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): 3–4 [interactive]. [accessed on 15-06-2013]. <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf>.

6 Giannopoulou, A. Copyright Enforcement Measures: The Role of the ISPs and the Respect of the Principle of Proportionality. *European Journal for Law and Technology*. 2012, 1(3) [interactive]. [accessed on 15-06-2013]. <<http://ejlt.org/article/view/Article/122/204>>.

7 Internet Blocking: Balancing Cybercrime Responses in Democratic Societies Study. October, 2009 [interactive]. [accessed on 15-06-2013]. <http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf>.

5. filtering for an unlimited period, which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work, in respect of which the applicant claims to hold intellectual-property rights, with a view to blocking the transfer of files, the sharing of which infringes copyright.

The same principles were also extended to hosting service providers in the most recent CJEU *Netlog* case C-360/10 decision.

The CJEU *Scarlet Extended* decision expressly reiterated that IP addresses are personal data, which shall be subject to data protection laws, and cannot be controlled (collected, analysed, etc.), without complying with the data controller obligations. It was elegantly laid down by the CJEU in the C-275/06 *Promusicae v. Telefonica* case, the protection of intellectual property must be balanced against the protection of the fundamental rights of individuals, which would be affected. In this earlier case, the CJEU established strict requirements for when online subscriber's privacy can be compromised (his identity disclosed based on IP address)⁸.

These CJEU cases demonstrate that Internet filtering and enforcement online indeed faces a maze of fundamental rights issues, which cannot be easily overcome. *Scarlet Extended/Netlog* and *Promusicae* conditions are difficult to meet and, especially in case of non-corporate right holders, may make the remedies overall inaccessible. Even in case of collecting societies and other corporate right holders, these remedies become of limited utility and may even be counterproductive. In the Netherlands, the ISPs implementing the IP and DNS blockade of the Pirate Bay⁹ have reported that P2P traffic has not abated but increased, following the blockade¹⁰, while it took several expensive and lengthy court cases (beginning in 2005) to achieve that the said Dutch ISPs comply with this blockade. It is notable that the CJEU *Scarlet Extended/Netlog* decisions are rather recent and conditions set in them have not yet filtered into the national case law, and it remains to be seen how they will be interpreted and implemented in the future.

In addition to the "three strikes" and filtering/blocking approaches being problematic from the privacy and freedom of expression standpoints, they are also only relatively successful in tackling the IPR infringement at the individual level¹¹. Individuals directly unaffected by the remedy are influenced only circumlocutory, through fear of similar sanctions applied to them and often disregard it¹². From a socio-legal perspective,

8 Coudert, F.; Werkers, E. In *The Aftermath of the Promusicae Case: How to Strike the Balance?* *Int J Law Info Tech.* 2010, 18(1): 50–71.

9 De pagina die u probeert te bereiken is op last van de rechter onbereikbaar gemaakt [interactive]. [accessed on 04-07-2013]. <<http://www.xs4all.nl/geblokkeerd/>>.

10 Torrents toegenomen sinds blokkade Pirate Bay. 4 July, 2012 [interactive]. [accessed on 04-07-2013]. <<https://blog.xs4all.nl/2012/07/04/torrents-toegenomen-sinds-blokkade-pirate-bay/>>.

11 Meyer, T. Graduated Response in France: The Clash of Copyright and the Internet. *Journal of Information Policy.* 2012, 2: 107–127 [interactive]. [accessed on 01-07-2013]. <<http://jip.vhost.psu.edu/ojs/index.php/jip/article/download/71/54>>.

12 Peukert, A. *Why Do 'Good People' Disregard Copyright on the Internet?* 2010 [interactive]. [accessed on 01-07-2013]. <http://www.jura.uni-frankfurt.de/ifrv1/peukert/forschung/Peukert_why_do_good_people_disregard_copyright_on_the_internet_.pdf>.

both “three strikes” and filtering/blocking do not offer a final resolution – they do not eliminate the source of the illicit content – and assuming the current socio-economic environment, there is hardly any further remedies available (save for the imprisonment) for most subscribers, if they fail to discontinue illicit content downloading and sharing.

Both “three strikes” and filtering/blocking have adverse effect on the legal Internet content, unsuspecting Internet users or even the society at large. This is due to necessary technical interference with the flow of information (monitoring and logging of IP addresses, and resources accessed by the subscribers behind these IP addresses). The importance of free flow of information online was proved decisively during the Arab Spring events. Even limited filtering of non-illicit content may be extremely damaging and easily abused for political or economic purposes. Filtering/blocking technologies implemented at ISP level are also technically challenging and expensive. This is especially applicable to sophisticated DPI technologies, which also cause grave privacy concerns (it directly implements censorship of the content accessed by the individual or individuals). All blocking and filtering technologies implemented at the ISP level also adversely affect the reliability and speed of the networks – filter may well be the bottleneck of the network¹³. It must be clearly acknowledged that the costs of implementing either of these measures is passed on all Internet users (included in the cost of the Internet access), hence, it hinders Internet access for legitimate users. Costs of implementing filtering/blocking instruments may also have negative effects on the competition in online services, since smaller service providers may be squeezed out of the market.

From a technical perspective, Internet filtering can be easily overcome through proxy or VPN servers. For ISPs (and their legitimate user base), this is yet another unwelcome trend, since it burdens the Internet infrastructure with inefficient and expensive foreign proxy traffic, i.e., produces collateral damage for all users of the ISP and accessing the Internet for other purposes than downloading of illicit content.

All of this suggests that current remedies aimed at online content are ill suited to deal with online infringements.

2. Perspective on available remedies

The bulk of available remedies for intellectual property rights infringement are carried over from the general civil procedure and are dependent on three key features:

- known infringers;
- explicit evidence; and
- parties, which can be easily reached in terms of procedural law.

Principal legal instruments for enforcing intellectual property online in the European Union to date rely on the EU Enforcement Directive. The Enforcement Directive

13 Lennett, B. Dis-Empowering Users vs. Maintaining Internet Freedom: Network Management and Quality of Service (QoS). *CommLaw Conspectus*. 2009 (18): 97–147 [interactive]. [accessed on 04-07-2013]. <<http://commlaw.cua.edu/articles/v18/18.1/06.Lennett.Final.pdf>>.

required all Member States to apply effective, dissuasive and proportionate remedies and penalties against those engaged in counterfeiting and piracy, and promoted availability of the remedies to right holders in the EU. Unfortunately, despite the positive role of the EU Enforcement Directive, it introduced very few new remedies (publicity, access to evidence), while retaining the limitations of the above three premises. Essentially, the Enforcement Directive provides for the “offline” remedies. In a context of ever changing online environment, such remedies are too slow, too complex and too expensive. Many critics of the Enforcement Directive have mentioned that it provides little help for small right holders, which struggle with the complexity of the national legal systems, time and financial expenses required to defend their rights¹⁴. This is even more applicable to the Internet, where chances for a retribution are often bleak.

In an online environment, the enforcement of intellectual property rights most often faces an unknown infringer (identifiable only through aliases, such as IP address, domain name, proxy address, etc.) and indirect and ephemeral evidence. It is not infrequent that the perpetrator and/or pertinent online resources are located in jurisdiction, which is outside of the reach of the rights-holder. The latter is becoming a dominant trend in the EU.

As a result, the existing set of remedies is insufficient for the global digital challenges to intellectual property rights. Even provisional and precautionary measures often sought in practice are ineffective against online resources, especially when they are located in foreign jurisdictions, which have limited regard for intellectual property rights. Thus, currently available remedies provide no instruments, which would deter the infringement and resolve the situation, when the infringement has happened.

It is important to emphasize that available remedies under the Enforcement Directive and pertinent national law allow pursuit against the consumers of the illicit online content, but offer no means to deal with the source of IPR infringements online – professional parties (P2P network operators) profiting from content sharing. This is also applicable to the newer “three strikes” and filtering/blocking remedies, which target users and service providers, but not the source of the illicit online content. Even right-holder groups (BREIN) acknowledge that online “piracy is mostly about illegal distribution”, therefore, principal problems are caused by “the limited number of sites that are either infringing or facilitating infringements” and which “should be the main focus of enforcement actions”¹⁵.

All abovementioned facts highlight the need for novel remedies, which would address on the said “offline” limitations and refocus the remedies from subscribers to the source of the illicit content online. The novel remedies shall be available in parallel to the existing ones, rather than replacing them.

14 Harhoff, D. *Challenges Affecting the Use and Enforcement of Intellectual Property Rights*. 2009 [interactive]. [accessed on 05-07-2013]. <<http://extwww.patent.gov.uk/ipresearch-challenges-200905.pdf>>.

15 Report on Commission/Presidency Conference of 26 April 2012 on the Enforcement of Intellectual Property Rights: The Review of Directive 2004/48/EC, AF/na - ARES (2012) 712109: 12 [interactive]. [accessed on 05-07-2013]. <http://ec.europa.eu/internal_market/iprenforcement/docs/conference20120426/summary_en.pdf>.

3. Rare success in enforcing intellectual property online

It is surprising that some of the successes of protecting intellectual property online are not employed for broader use. Cybersquatting problem, which plagued the Internet in the nineties, before P2P technologies even existed, was effectively tamed not by harsh remedies, but by the novel online alternative dispute resolution approach enforced supranationally through the administrators of the domain name system (DNS) – the Internet Corporation for Assigned Names and Numbers (ICANN) and domain registrars. The UDRP is a process for the resolution of disputes regarding the registration of Internet domain names. The UDRP currently applies to all .aero, .asia, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .pro, .tel and .travel top-level domains, and some country code top-level domains, including .eu. Currently, 65 country-code top-level domains (ccTLDs) have adopted the UDRP or a variation thereof and fall under the UDRP procedure administered by the WIPO Arbitration and Mediation Center¹⁶.

When an interested party (registrant) applies to register a domain name, the registrant must, among other things, accept (as part of the Terms and Conditions) that the applied for the domain name “*will not infringe upon or otherwise violate the rights of any third party*”, and agree to accept the UDRP procedure, if any third party claims violations of rights, including intellectual property rights.

It is noteworthy that the domain name system (DNS) remains essentially the most centralized backbone part of the Internet, centrally governed by the ICANN and a limited number of top level domain registrars. With the pending 2013 expansion of the top level domain names, the UDRP will extend, as well.

Based on the UDRP, the ultimate ownership (transfer thereof) of the domain names is decided. Any affected party (trademark owner) may initiate the UDRP procedure. Being administrative, the UDRP procedure is optional for trademark owners, but mandatory for top-level domain name registrars and registrants (parties, who have registered the domain name). The UDRP does not prevent either party from submitting a dispute to a national court of competent jurisdiction; but very few cases that have been decided under the UDRP have been brought before national courts¹⁷. If a domain name registrant loses a UDRP proceeding, he must file a lawsuit against the trademark holder within ten days to prevent the automatic transferring of the domain name. In essence, the UDRP has established a completely novel kind of remedy – seizure of online resource – domain name – in order to remedy illicit use of such domain name for trademark infringement.

Since its establishment in 1999, the UDRP has proven to be highly popular among trademark owners and established itself as the primary process to deal with cybersquatting of the top-level domains that it deals with. According to WIPO Arbitration and

16 Domain Name Dispute Resolution Service for Country Code Top Level Domains (ccTLDs) [interactive]. [accessed on 15-06-2013]. <<http://www.wipo.int/amc/en/domains/ccTld/index.html>>.

17 The Uniform Domain Name Dispute Resolution Policy and WIPO. August, 2011 [interactive]. [accessed on 15-06-2013]. <<http://www.wipo.int/export/sites/www/amc/en/docs/wipointaudrp.pdf>>.

Mediation Center, “the UDRP has long been offering an effective solution for trademark owners, domain name registrants, and registration authorities. Introduced to meet the need for an administrative dispute resolution mechanism purpose-designed to resolve certain trademark-based online conflicts occurring across national jurisdictions while retaining court options, it has won international respect as an expedient alternative to those court options.”¹⁸ Despite criticism and call for improvement, it is also generally favorably regarded by intellectual property scholars as a rare case of relatively successful enforcement of intellectual property rights online¹⁹. The UDRP is also deemed as the only proven mechanism in place to absorb the impact of gTLD expansion²⁰.

The UDRP procedure offers major procedural advantages, compared to the national judicial procedures. It is a streamlined – very fast and relatively inexpensive – procedure. Cases are decided by specialized intellectual property law experts, rather than general competence judges, the body of UDRP arbitrators is international, free from political influences and governmental complexities.

The author believes that domain seizure through the UDRP also owns its success to addressing the three “offline” limitations of the traditional remedies, i.e., the UDRP effectively deals with the unknown party and foreign jurisdiction problems. The UDRP and domain seizure remedy are aimed directly at the infringer, rather than at the unknown and anonymous party. Domain name, which is used for illicit activities, is very close to the source of the infringement and may even be directly owned by the source. Collateral damage produced by the domain seizure is also relatively controlled, especially when compared – it does not (or minimally) affect the ISPs and does not affect public at large, does not increase the costs of online services and very rarely threatens legitimate Internet content (e.g., several websites under one IP). For *prima facie* infringement cases, it may offer almost immediate resolution with little effort on the side of the rights holder.

The UDRP has obvious limitations: it does not address the damage issues, it still bears some costs, which are non-recoverable, it does not in itself address the difficult jurisdiction issue (it is possible for the perpetrator to switch to another domain with minimal disruption) and it is currently limited to trademark law and closely related disputes.

Starting in 2010, the US have pioneered government led domain name seizures as a new remedy for tackling unlawful acts (including copyright infringement) online, however, the procedure has been applied by the government agencies in mainly criminal procedures and towards the registrars of the TLDs within the national jurisdiction (e.g., Verisign Inc., which is the root registrar of all .com TLDs). The most prominent cases, where the US have exercised this, include one of the top P2P file sharing websites, Torrent-Finder.com, as well as top online gambling portal pokerstars.com, which was accused of money laundering and other illicit activities online, and later settled the

18 *Ibid.*

19 Moore, M. Cybersquatting: Prevention Better than Cure? *Int J Law Info Tech.* 2009, 17(2): 220–231.

20 Harhoff, D. *Challenges Affecting the Use and Enforcement of Intellectual Property Rights.* 2009 [interactive]. [accessed on 05-07-2013]. <<http://extwww.patent.gov.uk/ipresearch-challenges-200905.pdf>>.

dispute. In case of Torrent-Finder.com, the domain was seized permanently. Another, prominent P2P tracker website demonoid.com, as a result, has jumped to demonoid.me domain for its main operations. The same has recently happened with The Pirate Bay principal .com domain name, which is now forwarded to .se website.

While domain seizure may be an effective remedy (albeit with the said limitations), it may be used non-optimally when it is in the hands of the national governments. Government reliant domain seizure suffers from the same substantive and procedural issues as most judicial remedies. It should be noted that the seizure shall be ordered by the court, based on the request and evidence produced by the competent authorities. Thus, it may suffer from the lack of specific intellectual property law expertise, complexity of procedure, time and financial expense, as well as political interference. Some domain seizures, e.g., domains cuba-hemingway.com, cuba-havanacity.com, ciaocuba.com, bonjourcuba.com, which were seized, but later reinstated by the US authorities, do raise legitimate concerns²¹ about the “digital Guantanamo” and unilateral exercise of power against the important backbone part of the Internet.

4. UDRP process for copyright infringements?

The author proposes to extend the existing UDRP process and institutions to a greater use for intellectual property rights holders, enabling it to make domain name seizure and take-over available to anyone, whose copyright or related rights are affected by the use of the domain name, or Internet resources available under (or associated with) the domain name.

The extension may be implemented at the national level, through adoption of the domain forwarding (temporary seizure) as an interim remedy, and domain takeover (permanent seizure) as the final remedy in the civil procedure. Such extension would be easy in a way that it will not require any legislative modifications and in most jurisdictions, including Lithuania, it can be implemented through judicial precedent. On the other hand, its effectiveness would be limited, since it would succumb to the traditional problems of the judicial procedure, highlighted previously, and would have strictly national effect.

Another way of extension would be international bound extension through the UDRP system. UDRP institutions have amassed substantial expertise and precedent in establishing illicit use of domain names, which take into account the content of the interned resources available under (or associated with) the domain name. The UDRP procedures rely on the intellectual property law experts, contrary to the national general competence judiciaries, which are struggling with the lack of special expertise needed to deal with the complex digital copyright and related rights issues. As it was noted, the

21 Liptak, A. *A Wave of the Watch List, and Speech Disappears*. March 4, 2012 [interactive]. [accessed on 15-06-2013]. <http://www.nytimes.com/2008/03/04/us/04bar.html?_r=1>.

UDRP also possesses a significant benefit of low enforcement expenses and very hasty procedure (compared to general judicial process).

Obviously, domain seizure under the UDRP procedure for copyright and related rights infringements as it stands will have some major limitations for its application in copyright and related rights infringement, including:

- no possibility to deal with many country level TLDs;
- no possibility to deal with domain forwarding situations, i.e., where .com domain is forwarded to a country domain (demonoid.com → demonoid.me; thepiratebay.com → thepiratebay.se), and therefore, the domain only indirectly contributes to infringement;
- domain seizure is not an uncircumventable solution, especially since domain names can be avoided in accessing infringing resources (through IP address based access).

The above limitations are generally applicable for any current blocking/filtering technologies, hence, given the advantages, the proposed remedy is of additional utility compared to available remedies.

Nevertheless, domain seizure under the UDRP procedure for copyright and related rights infringements may be just the right tool against “the limited number of sites that are either infringing or facilitating infringements”. It would allow certain marginalization of P2P and other infringing sites, especially if supported by the search engines. For the search engines, UDRP awards shall serve as the legal basis and simple red-flagging means for eliminating certain content from the search results. It shall be reminded that it would augment existing remedies rather than supplant them.

Domain seizure under the UDRP approach would be a preferred remedy from the point of view of the public and the online service providers, since it will not disrupt the general flow of information online, it would be much more selective compared to current blocking and filtering technologies, the economic costs to implement it would be marginal (especially compared to expensive technologies, such as DPI filtering) and it would greatly benefit from existing specific expertise and precedent at the UDRP institutions. This new remedy would be principally compatible with the general subscriber privacy.

Adapting existing UDRP institutions to deal with any kind of IPR infringement under the domain name would not require major substantive legal framework, and it may be integrated into existing UDRP reform proposals²². The principal change needed is the new international (ICANN/WIPO) entitlement framework allowing domain name seizure (forwarding/takeover) for copyright and related rights infringing activities carried under the domain name (or associated therewith). The contributory infringement doctrine in case of domain names also needs development and formalization. A further step may be extending the procedure internationally and ensuring cooperation of the

22 Roy, A. Reflections on the Uniform Domain Name Dispute Resolution Policy as It Enters Its Second Decade. *Int J of Technology Policy and Law*. 2012, 1(1): 15–24.

larger number of the national TLD registrars (which realistically may be achieved much faster than cooperation of individual Internet service providers, since domain registrars have no economic interests to protect). It is also very important to note that in case of domain registrars the number of parties is much lesser compared to billions of Internet subscribers and tens of thousands of service providers connected to the Internet. Cooperation of search providers may also be sought. The latter two steps would allow efficient dealing with the rogue jurisdictions, as well as domain forwarding.

Conclusions

The bulk of available remedies for intellectual property rights infringement are carried over from the general civil procedure and are characterized as “offline” remedies, which are poorly adapted to deal with the fast changing nature of intellectual property infringements online. The most recent remedies – “three strikes” and internet filtering/blocking – are moving online; however, they suffer from major limitations and are very difficult to balance with the fundamental rights. It must be recognized that they target not the source of the intellectual property infringements online - “the limited number of sites that are either infringing or facilitating infringements”, but instead they target individual subscribers, online service providers and through collateral damage – the general public. Thus, more targeted and more efficient online remedies are needed.

Overall, success in efficiently enforcing intellectual property rights online is rare. One case of such success is the UDRP procedure, which deals with cybersquatting, i.e., infringement of trademark rights in domain names. The UDRP has developed into expertly administered, streamlined, fast and inexpensive process, which allows seizure and takeover of infringing domains and also takes into account the contents of the Internet resources available under the claimed domain. A significant body of precedent and institutional infrastructure supports the UDRP as the primary way to resolve conflicts on the principal TLDs, as well as all new TLDs coming later this year.

The author proposes to extend the existing UDRP process and institutions to a greater use for intellectual property rights holders, enabling it to make domain name seizure and take-over available to anyone, whose copyright or related rights are affected by the use of the domain name, or Internet resources available under (or associated with) the domain name. Such new remedy would be efficient, targeted and much less adverse to fundamental rights, while at the same time focused on the source of illicit digital content. While not without limitations, it would allow certain marginalization of P2P and other infringing sites. The proposal may be implemented through the new international (ICANN/WIPO) framework, which may also be included into the UDRP reform proposals, which are currently circulating.

References

- Liptak, A. *A Wave of the Watch List, and Speech Disappears*. March 4, 2012 [interactive]. [accessed on 15-06-2013]. <http://www.nytimes.com/2008/03/04/us/04bar.html?_r=1>.
- Roy, A. Reflections on the Uniform Domain Name Dispute Resolution Policy as It Enters Its Second Decade. *Int J of Technology Policy and Law*. 2012, 1(1):15–24.
- Domain Name Dispute Resolution Service for Country Code Top Level Domains (ccTLDs) [interactive]. [accessed on 15-06-2013]. <<http://www.wipo.int/amc/en/domains/cctld/index.html>>.
- Moore, M. Cybersquatting: Prevention Better than Cure? *Int J Law Info Tech*. 2009, 17(2): 220–231.
- The Uniform Domain Name Dispute Resolution Policy and WIPO. August, 2011 [interactive]. [accessed on 15-06-2013]. <<http://www.wipo.int/export/sites/www/amc/en/docs/wipointaudrp.pdf>>.
- Peukert, A. *Why Do 'Good People' Disregard Copyright on the Internet?* 2010 [interactive]. [accessed on 01-07-2013]. <http://www.jura.uni-frankfurt.de/ifrv1/peukert/forschung/Peukert_why_do_good_people_disregard_copyright_on_the_internet_.pdf>.
- Giannopoulou, A. Copyright Enforcement Measures: The Role of the ISPs and the Respect of the Principle of Proportionality. *European Journal for Law and Technology*. 2012, 1(3) [interactive]. [accessed on 15-06-2013]. <<http://ejlt.org/article/viewArticle/122/204>>.
- Lennett, B. Dis-Empowering Users vs. Maintaining Internet Freedom: Network Management and Quality of Service (QoS). *CommLaw Conspectus*. 2009, (18): 97–147 [interactive]. [accessed on 04-07-2013]. <<http://commlaw.cua.edu/articles/v18/18.1/06.Lennett.Final.pdf>>.
- De pagina die u probeert te bereiken is op last van de rechter onbereikbaar gemaakt [interactive]. [accessed on 04-07-2013]. <<http://www.xs4all.nl/geblokkeerd/>>.
- Harhoff, D. Challenges Affecting the Use and Enforcement of Intellectual Property Rights. 2009 [interactive]. [accessed on 05-07-2013]. <<http://extwww.patent.gov.uk/ipresearch-challenges-200905.pdf>>.
- Coudert, F.; Werkers, E. In the Aftermath of the Promusicae Case: How to Strike the Balance? *Int J Law Info Tech*. 2010, 18(1): 50–71.
- Brown, I. Internet Self-Regulation and Fundamental Rights. *Index on Censorship*. March 2010, (1) [interactive]. [accessed on 15-06-2013]. <<http://ssrn.com/abstract=1539942>>.
- Internet Blocking: Balancing Cybercrime Responses in Democratic Societies Study. October, 2009 [interactive]. [accessed on 15-06-2013]. <http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf>.
- Lemley, M. A.; Reese, R. A. Reducing Digital Copyright Infringement without Restricting Innovation. *Stanford Law Review*. 2004, 56(1345) [interactive]. [accessed on 15-06-2013]. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=525662>.
- Kiškis, M.; Petrauskas, R. Intelektinės nuosavybės elektroninėje erdvėje pažeidimų ypatumai. *Jurisprudencija*. 2006, 5(83): 29–36.
- 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): 3–4 [interactive]. [accessed on 15-06-2013]. <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf>.
- Report on Commission/Presidency Conference of 26 April 2012 on the Enforcement of Intellectual Property Rights: The Review of Directive 2004/48/EC, AF/na - ARES (2012) 712109: 12 [interactive]. [accessed on 05-07-2013]. <http://ec.europa.eu/internal_market/iprenforcement/docs/conference20120426/summary_en.pdf>.
- Torrents toegenomen sinds blokkade Pirate Bay. 4 July, 2012 [interactive]. [accessed on 04-07-2013]. <<https://blog.xs4all.nl/2012/>>

07/04/torrents-toegenomen-sinds-blokkade-pirate-bay/>
 Meyer, T. Graduated Response in France: The Clash of Copyright and the Internet. *Journal of Information Policy*. 2012, 2: 107–127 [interactive]. [accessed on 01-07-2013].

<<http://jip.vhost.psu.edu/ojs/index.php/jip/article/download/71/54>>.
 Mizaras, V. Intelektinės nuosavybės teisių gynimo reglamentavimo novelos Europos Bendrijos teisėje: pagrindiniai principai. *Teisė*. 2005, 55: 95–118.

NAUJOS TEISINĖS ATSAKOMYBĖS PRIEMONĖS KOVOJANT SU INTELEKTINĖS NUOSAVYBĖS TEISIŲ PAŽEIDIMAIŠ ELEKTRONINĖJE ERDVĖJE

Mindaugas Kiškis

Mykolo Romerio universitetas, Lietuva

Anotacija. Straipsnyje nagrinėjamas tradicinių teisinės atsakomybės priemonių nepakankamumas kovojant su intelektinės nuosavybės teisių pažeidimais elektroninėje erdvėje. Analizuojamas interneto domenų vardų priverstinis nukreipimas ir perdavimas. Siūloma perimti šią specialiąją sankciją į bendrą teisminę teisinės atsakomybės priemonių arsenalą ir išplėsti UDRP sistemą platesniam labiausiai paplitusių autorių teisių ir gretutinių teisių pažeidimų užkardymui internete. Ši priemonė padėtų pažeidimus marginalizuoti bent jau nacionaliniu mastu.

Reikšminiai žodžiai: teisinė atsakomybė, intelektinės nuosavybės teisių pažeidimas, alternatyvus ginčų nagrinėjimas, domenų vardai.

Summary. The paper explores the failure of traditional civil remedies, as well as newer “three strikes” and Internet filtering remedies, to tackle intellectual property rights infringement on the Internet. Although the “three strikes” and Internet filtering/blocking measures were introduced in response to inadequacy of traditional remedies, over the decade of practical applications they have not achieved significant success, as well.

Principal socio-legal reasons for such failures are reviewed and analyzed. Main reasons are found to be that traditional remedies and first generation new remedies are tailored to “offline” environment. Existing remedies are more suited to traditional legal interactions, where the parties are clearly identifiable and jurisdictional collisions are well defined. The way of action of existing remedies is inherently offline. They are ill adapted to the requirements of the online environment, such as difficulty to identify anonymous parties in multiple jurisdictions, and hence, high enforcement costs, as well as legal and technological complexity. It should be noted that online environment requires swift enforcement in view of the dynamic technological change. Based on this analysis, key features of the efficient online remedy design are identified.

In the second part of the paper, a case study of successful enforcement of trademark

rights online is presented. Example of rare success in enforcing legal liability for infringement of intellectual property rights is the special remedy of domain name seizure and take-over, implemented through the alternative and online dispute resolution procedure – the Uniform Domain Name Dispute Resolution Policy (UDRP). Domain seizure/takeover remedy implemented through the existing UDRP system works at the supranational level and successfully operates as an online instrument dealing with trademark rights infringement in the domain names. The author considers expansion of this special remedy and the domain seizure through the UDRP to cover copyright and related rights infringement as a viable addition to the existing remedies for the rights holders to deal with the online infringements. The former (that is a special sanction of domain seizure and take-over) may be relatively easily adopted by the judiciary both as an interim measure and as a final remedy; however, this would address only part of the challenges that enforcement of intellectual property rights faces online. Only the combination of the special sanctions and the online dispute resolution mechanism, capable to enforce such sanctions, address most inadequacies of traditional offline remedies (especially high cost, slowness and complexity, competence of the dispute resolution authority, as well as risks of political and legal abuses). This may be achieved through expansion of the existing UDRP system; however, it may need an additional supranational legal framework.

The paper recognizes limitations of any rights enforcement instruments online, which are predefined by the nature of the online environment – its extraterritorial nature and span over jurisdictions, which may willingly tolerate infringement of intellectual property rights. These limitations would set the limits over the effectiveness of the novel remedies.

Nevertheless, the domain seizure and take-over sanction made available for other infringements of the intellectual property rights online (chiefly copyright and related rights infringement) and enforced through relatively easily expandable UDRP system would complement the existing offline remedies and would expand the enforcement instrumentary for the rights holders, thus, enabling marginalization of the most popular intellectual property rights infringements online.

Keywords: remedies, intellectual property infringement, alternative dispute resolution, domain names.

Mindaugas Kiškis, Mykolo Romerio universiteto Socialinių technologijų fakulteto Skaitmeninių technologijų instituto profesorius, socialinių mokslų (teisė) daktaras. Mokslinių tyrimų kryptys: technologijų teisė, technologinio verslo teisė, intelektinė nuosavybė, inovacijos ir verslumas.

Mindaugas Kiškis, Mykolas Romeris University, Social Technologies Faculty, Institute of Digital Technologies, Doctor of Social Sciences (Law), Professor. Research interests: technology law, technology business law, intellectual property, innovation and entrepreneurship.