

## REVERSE DOMAIN HIJACKING

FAHED.W<sup>1\*</sup>

<sup>\*1</sup>Debrecen university hungary Legal researcher: [fahedw@yandex.com](mailto:fahedw@yandex.com)

**\*Corresponding Author: -**

Email: [fahedw@yandex.com](mailto:fahedw@yandex.com)

---

### **Prologue: -**

*There is often a conflict between domain names owners and trademarks holders' rights, and If a party has a specific domain name but the other party owns trademark rights with that name, it's likely that there's a problem, one of these problems presented by domain names hijacking.*

*From a legal perspective, domain names hijacking taking important place in cyberspace challenges, in this scenario, domain names rights are infringed when a third party managed to transfer a domain name to his account without illegal right to be able to resell it and gain money*

### **Assumption: -**

*The point of this research arises from that UDPR policy is not enough to solve the reverse domain hijacking phenomena, and then comprehensive legislation is needed to solve this phenomenon.*

### **Methodology: -**

*The methodology will depend on inductive approach based on Selected and analyses court decisions with legal texts. This paper will try to provides scholarly appraisal of the legal and policy related to domain names hijacking*

**Keywords: -** domain names, hijacking, Reverse hijacking, RDNH, ACPA



**research plan** this short paper will try to address some issues like:

- Definition of Reverse domain hijacking,
- mechanism of Reverse domain hijacking,
- Anticybersquatting Consumer Protection Act
- UDRP restrictions on reverse domain name hijacking
- Lanham act
- effects of Reverse domain hijacking,

### **List of Abbreviations**

- RDNH: Reverse Domain Name Hijacking Information.
- UDRP: Uniform Domain Name Dispute Resolution Policy
- TLD: top level domain names
- ICANN: The Internet Corporation for Assigned Names and Numbers
- WIPO: World Intellectual Property Organization
- ACPA: the Anticybersquatting Consumer Protection Act

### **1. Definition of Reverse domain names hijacking**

The practical practice of famous companies' trademarks registering, and keep them for specific time to achieve profit after reselling them<sup>1</sup>. The financial motivation is the most one behind domain names hijacking<sup>2</sup> millions of dollars of domain names are at risk as a result of this new source of profit, thus, there has been a sharp increase in reverse domain names hijacking<sup>3</sup> domain names hijacking defined as the illegal seizure of domain names by Change the domain name registration without the original registered permission, and this happened by first blocking access to the domain's DNS server then putting his own server up in its place<sup>4</sup> domain names hijacking (also known as reverse cybersquatting or commonly abbreviated as 'RDNH') Cybersquatting involves registering a domain name corresponding with someone else's name or mark with the intent to sell it at profit<sup>5</sup> as well defined as "is the practice of registering and using a well-known name or trademark as a domain to keep it away from its owner or to extort a substantial profit from the owner"<sup>6</sup>. however, Cybersquatting differs from ordinary trademark infringement because cybersquatters do not use domain names to sell products or services. The purpose of cybersquatting is to extract a payment from the owner of the trademark. And this makes Cybersquatting different from cyberpiracy which is related to copyright violation in website, while Cybersquatting is related to domain names' registration violations<sup>8</sup>

### **2. Mechanism of Reverse domain hijacking**

as it has mentioned that type of disputes arising over the rights to the domain name on traditional trademark principles,<sup>9</sup> The mechanism of Reverse domain hijacking is presented by registration or use of a trademark as a domain name in bad faith its concluded that trademark should be use as domain name only, and that using should be in bad faith but without permission of the original owners.

Usually, the domain name owner is given the right to transfer access or use this domain by The Domain Name Service Agreement<sup>11</sup> such these rights can be compromised the trademark's owners unequivocally exercise the Reverse domain name hijacking by taking advantage of their commercial rights to seize domain names from legitimate owners This desirability of the '.com' TLD has led to the practice of domain name hijacking

By this way a rightful trademark owner attempts to secure a domain name by making cybersquatting claims against a domain name's "cybersquatters" owner to take a domain name from a legitimate good faith domain names' owner the Anticybersquatting Consumer Protection Act, explain this mechanism by considering registering, trafficking in, or using a website domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else.

### **3. UDRP restrictions on reverse domain name hijacking**

The UDRP Policy Rules specify the hijacking of a reverse domain name in a bad faith complaint resulting in abuse of the UDRP management process. it also creates a cause of action for reverse domain name hijacking against trademark owners who misuse or abuse their rights

It becomes objectively difficult to identify what constitutes a subjective "bad faith", often leading to the actual contradictions of the parties as undetermined or intangible at best. Therefore, despite its clear recognition of the UDRP policy, the discovery of domain name hijacking is rare because Reverse domain name hijacking is found only in exceptional circumstances where the trademark owner can make<sup>21</sup>

#### **3.1 Bad faith matter**

Reverse domain name hijacking' is defined by paragraph 1 of the UDRP Rules to mean using the UDRP in bad faith to attempt to deprive a registered domain-name holder of a domain name<sup>22</sup>

It may be concluded that the bad faith principle is inherently controversial and difficult to approve, that's why in many legal stable areas, the courts abandoned efforts to regulate a bad faith<sup>23</sup>. the reason behind this is that it is very difficult to prove bad faith because it involves proving something about the state of decision maker's mind<sup>24</sup>, as well as it is impossible to anticipate all of the possible fact patterns related to bad faith<sup>25</sup>

This is difficult in any case, but more difficult in two respects. First, the decision itself is often within legal limits. Second, it is always easy for a dishonest decision-maker to provide reasonable justification, to make up his illegal decision<sup>26</sup>

However, Domain name owner is considered to be acting in bad faith when registering another's well-known trademark for commercial purposes<sup>27</sup> NSI placed the burden on the applicant to act in good faith in requesting a domain name<sup>28</sup>

The UDRP stipulated three substantive matter of reverse domain names hijacking: (1) that the disputed domain name is identical or confusingly similar to the mark;<sup>29</sup> (2) that the domain name registrant has no rights or legitimate interest in the domain name;<sup>30</sup> and (3) that the domain name has been registered and has been used in bad faith<sup>31</sup>. only if the Complainant proves that the registration was undertaken in bad faith<sup>32</sup> and the respondent has to prove that the domain name has been registered in good faith<sup>33</sup>

In the case of DIGITI limited liability company v. Privacy Administrator, Anonymize, Inc / Michele Dinoia, Macrosten LTD , the administrative panel of WIPO Arbitration and Mediation Center required that the Complainant must satisfy the Panel, in respect of the Disputed Domain Name that: the Disputed Domain Name is identical with or confusingly similar to a trademark or service mark in which the Complainant has rights; and The Respondent has no rights or legitimate interests in respect of the Disputed Domain Name; and The Disputed Domain Name has been registered and is being used in bad faith<sup>34</sup>.

As for bad faith The ICANN has identified the following actions as examples of bad faith:

- (1) evidence of efforts to extract payments for use of the domain name<sup>35</sup>.
- (2) evidence of registration as part of an attempt to prevent the owner from using his mark as a domain name and evidence of a pattern of such conduct<sup>36</sup>
- (3) evidence of registration as part of an effort to disrupt the mark owner's business; and (4) evidence that the domain name was used to divert commercial Internet traffic from the mark owner<sup>37</sup>.

One factor to consider is whether there is bad faith in the extent to which a trademark is used commercially prior to registration or the use of a domain name<sup>38</sup>.

Showing bad faith is not always an easy case as we mentioned above. For instance, Lady Gaga challenged an unauthorized user of the domain name, www.ladygaga.org, however, her claim was unsuccessful. The website involved in that case was a fan site promoting Lady Gaga. The National Arbitration Forum involved in this dispute decided that although the use of the domain was confusing and there was no legitimate right or interest on the part of the domain name user, this particular use as a fan site encouraged Lady Gaga doesn't constitute bad faith. If after considering the submissions, the Panel finds that the complaint was brought in bad faith, for example in an attempt at Reverse Domain Name Hijacking or was brought primarily to harass the domain-name holder, the Panel shall declare in its decision that the complaint was brought in bad faith and constitutes an abuse of the administrative proceeding. In case of DIGITI limited liability company v. Privacy Administrator, Anonymize, Inc Michele Dinoia, Macrosten LTD Found Guilty Of RDNH

A Belgium-based company has been found guilty of Reverse Domain Hijacking by a panel of the World Intellectual Property Organization, after the firm attempted to use the UDRP process to acquire the domain digiti.com. The domain is identical to a trademark owned by the company, although the domain, itself, was registered in 2002, while the trademark was only granted in 2018. And in case of Ville de Paris v. Jeff Walter Case, the Arbitration and Mediation Center of WIPO orders that the domain name <parvi.org> be transferred to the Complainant. The WIPO panel made specific note of the fact the domain registration preceded the trademark by 16 years, noting it is difficult to know whether the company filing the complaint even existed at the time of the domain registration. The complainant, the panel observed, filed no information about its own business, which, the panel wrote, contributed to its RDNH ruling. The panel wrote, "The Complainant seems to have assumed that because it has a registered trademark identical to the Disputed Domain Name, and the Disputed Domain Name was linked to a PPC webpage, it could file the briefest of complaints without any further supporting detail or useful information."

#### **4. ACPA restrictions on reverse domain name hijacking**

Before ACPA, there was no law that specifically made such this behavior illegal although Trademark and domain name disputes are among the oldest types of legal disputes on the Internet<sup>44</sup> however the ACPA is an extension of the Lanham Act which was passed by Congress in 1946, and codified the existing common law of trademarks. The Anticybersquatting Consumer Protection Act does not expressly recognize reverse domain name hijacking and often only limits defendants' recovery to retention or transference of the domain name.

It also fails to provide any remedies for victims of attempted reverse cybersquatting. However, the statute permits some monetary relief where bad faith, reckless disregard or the willful violation of a court order are involved. On the other hand, it creates a cause of action for reverse domain name hijacking against trademark owners who misuse or abuse their rights.<sup>47</sup>

The ACPA<sup>48</sup> expressly prohibits 'cybersquatting' or other forms of domain name speculation so some believe that Cybersquatting differs from ordinary trademark infringement because cybersquatters do not use domain names to sell products or services, the purpose of cybersquatting is extract payment from the owners of trademarks.<sup>49</sup> The cybersquatters seeks to register domain names in bad faith in order to extort a trademark owner<sup>50</sup>. the courts can enforce the rights of trademark owners if they prove that domain name make consumers feel confused between the goods or services of the registrar or the relationship between the entities<sup>51</sup>.

In this regard, a question arises as to whether the rights of domain names should be considered primarily as part of a property<sup>52</sup> or whether they can be considered as a contract<sup>53</sup>. Such this question has resulted to Opening the floodgates to

controversial and heat debate on the legal character of domain names, and then to reaching out the best way to solve any conflicting related to it.

Under the ACPA, it's a crime to register a domain name that is confusingly similar to the trademark or personal name of another, or to register a famous trademark as a domain name and then offer it for sale to the trademark owner. These kinds of extortionate behaviors are prohibited by the ACPA as "cybersquatting." Yet, principles of property law would define acts constituting cybersquatting differently than would principles of contract law.

On the other hand, viewed in light of contract law principles, registering a domain name creates a contract right, not a property right. Like any other contract, it must be entered in good faith.

Considering this fundamental contract principle, when an individual renews a domain name registration to keep that particular domain name for himself and, therefore, unavailable to anyone else, the individual's actions fall within the purview of the extortionist behavior that the ACPA was drafted to prohibit. The discussion section will then<sup>54</sup> dissect each approach to conclude that, in light of the intent to prevent extortion and unfair business practices that is apparent from the ACPA, the Third and Eleventh Circuits were correct to interpret rights to domain names under principles of contract law.<sup>55</sup> Some still argue that registrar of domain names and currently the largest, has seemed to concede that domain names are not service contracts, but intangible property<sup>56</sup>

## 5. Civil actions

Among other mechanism were suggested by WIPO to solve domain name conflicts, existing judicial action mechanism and establishing an accommodative dispute solving mechanism were believed to be proper solutions which came amid a years-long effort to curb reverse domain names hijacking<sup>57</sup>. however ICANN' s policy didn't try to solve issues that do not involve a bad-faith domain name holder<sup>58</sup>. While the UDRP is limited to cases of bad faith registration and use<sup>59</sup> with bearing in mind that UDRP panelists currently have no tools by which to punish abuses such as Reverse Domain Name Hijacking, such a finding might be used in a local jurisdiction where such abuses might constitute a tort such as tortious interference with contract or an unfair business practice.

A domain name registrant whose domain name has been suspended, disabled, or transferred under a policy described under clause (ii) the UDRP Policy may, upon notice to the mark owner, file a civil action to establish that the registration or use of the domain name by such registrant is not unlawful under this Act and it might be considered as unfair competition and deserve compensation<sup>60</sup>.

The court may also grant judicial compensation to the registrar of the domain name, including reinvigorating the domain name or transferring the domain name to the domain name registrar<sup>61</sup>.

### 5.1 Lanham Act

by analyzing Lanham act at 15 U.S.C. § 1117(d) we can find further protection related to statutory damages, it has mentioned that in cases "involving a violation of section 1125," an election of damages in the courts discretion of "not less than \$1,000 and not more than \$100,000 per domain name<sup>62</sup>, it was a quantum leaps to permit the plaintiff to have compensation for statutory damages equals \$100,000 per domain name in lieu of actual damage<sup>63</sup> .

In some cases, and based this law, the Domain names owners have successfully won damage awards in federal lawsuits under the ACPA in which the domain owner claimed that it was the victim of reverse domain name hijacking<sup>64</sup>. For example, the City of Paris was ordered to pay \$100,000 as a result of a RDNH finding for parvi.org in this case the law was clear that trademark holders may recover statutory damages between \$1,000 and \$100,000. This is a rational reason to a point due to the difficulty of proving that the violator can trig sufficient damage to make the federal suit applicable<sup>65</sup>. another example is presented by that GoForIt Entertainment was ordered to pay \$100,000 as a result of its RDNH attempt against Scott Day's Digimedia.com LP.

The owner of the MyArt.com domain name lost a UDRP on the domain. The domain owner then filed suit in Federal Court under the ACPA claiming that the UDRP Complaint was Reverse Domain Name Hijacking. The domain owner succeeding in obtaining an offer of judgment and monetary damages.

A finding of Reverse Domain Name Hijacking where a trading company buys up all the possible domain names that it could ever want, may also be the basis for bringing a cause of action at the US Patent and Trademark Office to cancel the trademark rights of the company that is asserting rights to the disputed domain under a provision that states that trademark rights may be cancelled if they are misused.

## 6. effects of Reverse domain hijacking

Neither the UDRP nor the ACPA provides much deterrent to curb trademark owners' abuse of their rights to abate reverse domain name hijacking practices, some argue even that the UDRP process would probably not be an appropriate solution because it would lengthen the dispute resolution processes<sup>66</sup>, as a result, reverse domain name hijacking can disrupt or severely affect the business and operations of the domain owner, including the denial and theft of email services, unauthorized disclosure of information through phishing and tapping sites<sup>67</sup>.

## Conclusions

- 1- reverse domain names hijacking depends on the factual circumstances surrounding each case.
- 2- reverse domain name hijacking can disrupt or severely affect the business.
- 3- Reverse domain name hijacking is related to using the UDRP rules in bad faith,

- 4- Neither the UDRP nor the ACPA provides much of protection in terms of reverse domain names hijacking cases, so the civil actions remain as crucial solutions in many cases.
- 5- Registered owners can protect themselves against hijacking by renewing their registrations in a timely fashion.
- 6- UDRP policy needs to be developed on legislative level to extend civil compensation.

## References

- [1].Orin Hargraves, *New Words*, Oxford University Press, 2004, P 70
- [2].Jerry Pournelle, Erin McKean, *1001 Computer Words You Need to Know*, Oxford University Press, 2004, p36.
- [3].Angus Stevenson, Maurice Waite, *Concise Oxford English Dictionary: Luxury Edition* Publisher OUP Oxford, 2011, p356.
- [4].Susie Dent, *The Language Report* Publisher Oxford University Press, 2003, Page 31.
- [5].Richard Lindsay, *Ad Law: The Essential Guide to Advertising Law and Regulation*, Kogan Page Publishers, 2016, P46,
- [6].Berkeley Technology Law, *Journal University of California Press*, 2005,2005 Volume 20, Issue 1 - Page 185.
- [7].James Van Roekel, MaryAnn Bell, Bobby Ezell, *Cybersins and Digital Good Deeds: A Book About Technology and Ethics*, CRC Press, 2006, p51.
- [8].What's in a Name: Reverse Domain Name Hijacking and Cybersquatting, <https://hutchersonlaw.com/reverse-domain-name-hijacking-cybersquatting>
- [9]. Nam H Nguyen, *2018 Essential Cyber Security Handbook in English*, Publisher am H Nguyen, 2018
- [10]. Jacqueline D. Lipton, *Internet Domain Names, Trademarks and Free Speech*, Publisher Edward Elgar Publishing, 2010, p12
- [11]. Munindar P. Singh, *The Practical Handbook of Internet Computing* Publisher CRC Press, 2004, p 1302
- [12]. Lee A. Bygrave, Jon Bing, *Internet Governance: Infrastructure and Institutions*, Publisher OUP Oxford, 2009, p82. Ibid, p 96
- [13]. *Journal of Legal Studies in Business - Volume 6*, Publisher West Publishing Company, 1999, Page 110.
- [14]. David Lindsay, *International Domain Name Law: ICANN and the UDRP*, Publisher Bloomsbury Publishing, 2007 p96
- [15]. *BNA's Banking Report - Volume 74* ,2000, Page 896.
- [16]. Emily Hurtt, What's in a Name? The Rights to Domain Names Under Various Principles, *University of Cincinnati Law Review* December 1, 2017 p840
- [17]. Emily Hurtt, What's in a Name? The Rights to Domain Names Under Various Principles, *University of Cincinnati Law Review* December 1, 2017 p840
- [18]. What's in a Name: Reverse Domain Name Hijacking and Cybersquatting, <https://hutchersonlaw.com/reverse-domain-name-hijacking-cybersquatting/>
- [19]. Bashir Ahmad Mallal, *The Malayan Law Journal*, Volume 2, Publisher Malaya Publishing House Limited, 2000 Page xix,
- [20]. Seymour Bosworth, M. E. Kabay, *Computer Security Handbook*. Publisher John Wiley & Sons, 2002 Page 10.
- [21]. *Congressional Record*, V. 145, Pt. 14, August 4, 1999 to August 5, 1999, p 20012.
- [22]. the United States federal law known as Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d), is a U.S. law enacted in 1999 that established a cause of action for registering, trafficking in, or using a domain name confusingly similar to, or dilutive of, a trademark or personal name.
- [23]. the UDRP Policy Rules Paragraph 15 (e)
- [24]. Adam V. Floyd, *O'Connor's Federal Intellectual Property Codes Plus*, Jones McClure Pub., 2007, p 60
- [25]. American Bar Association. Section of Public Utility, Communications, and Transportation Law, *Annual Report*, Publisher American Bar Association Section of Public Utility, Communications and Transportation Law, 2003, p201 Ibid
- [26]. United Nations Conference on Trade and Development, *E-Commerce and Development Report 2002*, p44.
- [27]. Raymond S. R. Ku, *Cyberspace Law: Cases and Materials*, Wolters Kluwer Law & Business, 2016, p290-291
- [28]. David Lindsay, *International Domain Name Law: ICANN and the UDR*, Bloomsbury Publishing, 2007, p161.
- [29]. Peter Luther & Alan Moran, *Technology in America*, Macmillan International Higher Education, 2018, p533.
- [30]. Vakul Sharma, *Information Technology Law and Practice*, Universal Law Publishing, 2011, p 531.
- [31]. Margaret Jane Radin, John A. Rothchild, Gregory M. Silverman, *Intellectual Property and the Internet: Cases and Materials*, Foundation Press, 2004, p180.
- [32]. Margaret Jane Radin, John Rothchild, Gregory M. Silverman, *Internet Commerce: The Emerging Legal Framework: Cases and Materials*, Publisher Foundation Press, 2002, p257.
- [33]. J. Thomas McCarthy, Roger E. Schechter, David J. Franklyn, *McCarthy's Desk Encyclopedia of Intellectual Property*, the University of Michigan, Publisher Bureau of National Affairs, 2004, p523.
- [34]. Harold C. Wegner, Edward G. Poplawski, *Understanding the new patent law: how the changes affect your patent practice and portfolio*, Publisher Practising Law Institute, 2000, p100.
- [35]. J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition Edition 4*, Publisher, Clark Boardman Callaghan, 1996, Volumes 1-7.
- [36]. Anthony Connerty, *A Manual of International Dispute Resolution*, Publisher Commonwealth Secretariat, 2006, p320.

- [37]. The John Marshall Journal of Computer & Information Law, Volume 22, Publisher John Marshall Law School, 2003, p644.
- [38]. Steve Hedley, Tanya Frances Aplin, Blackstone's Statutes [on] IT & E-commerce, Edition 2, Oxford University Press, 2004, p333.
- [39]. American Jurisprudence Pleading and Practice Forms Annotated: State and Federal, Volume 1, Part 3, Lawyers Co-operative Publishing Company Publisher, West Group 2000, p472.
- [40]. Practising Law Institute. Advanced Seminar on Trademark Law, Publisher Practising Law Institute, 2002, p 900.
- [41]. Annual Internet Law Institute - Volume 2, publisher Practising Law Institute, Page 230.
- [42]. Berkeley Technology Law Journal - Volume 15, Publisher University of California Press, 2000, Page 310
- [43]. Harvard Law Review: Volume 129, Number 4 – February, Quid Pro Books, 2016
- [44]. Christopher Enright, Federal Administrative Law, Federation Press, 2001, p393.
- [45]. Harvard Law Review, Volume 129, Number 4 – February, Quid Pro Books, 2016, ibid
- [46]. Christopher Enright, Federal Administrative Law, Federation Press, 2001, p393
- [47]. Graham Earnshaw, China Economic Review's China Business Guide 2005, Publisher SinoMedia (Holdings) Co. Ltd., p577.
- [48]. Michael D. Scott, Scott on Multimedia Law, Aspen Publishers Online, 2008, p 5-48
- [49]. United Nations Conference on Trade and Development, E-Commerce and Development Report 2002, p43.
- [50]. Jenny Ng, The Domain Name Registration System: Liberalization, Consumer Protection, and Growth, Publisher Routledge, 2013, p43 Ibid, p43
- [51]. Richard Raysman, Emerging Technologies and the Law: Forms and Analysis, Volume 1, Publisher Law Journal Press, 2002, p6-48
- [52]. Jenny Ng, The Domain Name Registration System: Liberalization, Consumer Protection, and Growth, Publisher Routledge, 2013, ibid, p43 Ibid p43
- [53]. Eun-Joo Min, WIPO Arbitration and Mediation Center, Mathias Lilleengen, Collection of WIPO Domain Name Panel Decisions, Publisher Kluwer Law International B.V., 2004 P15.
- [54]. Hector MacQueen, Charlotte Waelde, Graeme Laurie, Contemporary Intellectual Property: Law and Policy, Publisher OUP Oxford, 2010, p723.
- [55]. -Richard Raysman, Emerging Technologies and the Law: Forms and Analysis, Volume 1, Publisher Law Journal Press, 2002, p6-48
- [56]. David Lindsay, International Domain Name Law: ICANN and the UDRP, Bloomsbury Publishing, 2007, p 367
- [57]. DIGITI limited liability company v. Privacy Administrator, Anonymize, Inc / Michele Dinoia, Macrosten LTD Case No. D2018-2148, November 15, 2018
- [58]. Delta & Matsuura, Law of the Internet, 4th Edition - Volume 1, Publisher Wolters Kluwer Law & Business, 2016, P 12-38 Ibid, p12-38
- [59]. Delta & Matsuura, Law of the Internet, 4th Edition, Volume 1, Publisher, Wolters Kluwer Law & Business, ibid 2016 Page 12-38
- [60]. Delta & Matsuura, Law of the Internet, 4th Edition, Volume 1, Publisher, Wolters Kluwer Law & Business, 2016, ibid, p 12-38
- [61]. Delta & Matsuura, Law of the Internet, 4th Edition, Volume 1, Publisher, Wolters Kluwer Law & Business, 2016, ibid, p-34
- [62]. section 15(e) of the Rules for Uniform Domain Name Dispute Resolution Policy.
- [63]. Case Number: D2018-2148, <https://www.wipo.int/amc/es/domains/search/text.jsp?case=D2018-2148>
- [64]. Ville de Paris v. Jeff Walter, Case No. D2009-1278, WIPO Arbitration and Mediation Center, administrative panel decision, November 19, 2009, <https://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-1278.html>
- [65]. Computer Buyer's Guide and Handbook, University of Minnesota, Volume 20 publisher Computer Information Pub., 2001 1, University of Minnesota, Page 96
- [66]. Ibid, p96.
- [67]. Emily Hurtt, What's in a Name? The Rights to Domain Names Under Various Principles, University of Cincinnati Law Review December 1, 2017 p843
- [68]. Computer Law Reporter - Volume 38, Publisher Computer Law Reporter Incorporated, 2003, Page 824
- [69]. Adam V. Floyd, O'Connor's Federal Intellectual Property Codes Plus, Jones McClure Pub., 2007, p 60
- [70]. the ACPA is an extension of the Lanham Act which was passed by Congress in 1946, and codified the existing common law of trademarks.
- [71]. Lee A. Bygrave, Jon Bing, Internet Governance: Infrastructure and Institutions, Publisher OUP Oxford, 2009, p82
- [72]. Richard A. Spinello, A Defense of Intellectual Property Right Edward Elgar Publishing, 2009, p11,
- [73]. Preventive Law Reporter, Volume 18, 1999 Page 62.
- [74]. Gerald B. Halt, Jr., John C. Donch, J., Amber R. Stiles, Intellectual Property in Consumer Electronics, Software and Technology Startups, Publisher Springer Science & Business Media, 2013, p61.
- [75]. John G. Sprankling, The International Law of Property, Publisher OUP Oxford, 2014, p90.
- [76]. Konstantinos Komaitis, The Current State of Domain Name Regulation: Domain Names as Second-Class Citizens in a Mark-Dominated World, Publisher Routledge, 1st edition, 2010, p58.
- [77]. Journal of intellectual property law - Volume 11, the University of California, 2003, Page 128.
- [78]. Kentucky Law Journal - Volume 99, Issues 1-2, Publisher University of Kentucky, College of Law, 2010 Page 192.

- [79]. Konstantinos Komaitis, *The Current State of Domain Name Regulation: Domain Names as Second-Class Citizens in a Mark-Dominated World*, Publisher Routledge, 1st edition, 2010, *ibid*, p92.
- [80]. Emily Hurtt, *What's in a Name? The Rights to Domain Names Under Various Principles*, University of Cincinnati Law Review December 1, 2017 p840.
- [81]. Emily Hurtt, *What's in a Name? The Rights to Domain Names Under Various Principles*, University of Cincinnati Law Review December 1, 2017 p841
- [82]. *The Hastings Law Journal - Volume 56, Issues 1-3*, Hastings College of Law, 2005, Page 41
- [83]. Zheng Qin, *Introduction to E-commerce*, Springer Science & Business Media, 2010, P 186
- [84]. *Berkeley Technology Law Journal - Volume 15*, Publisher University of California Press, 2000, Page 310
- [85]. United Nations Conference on Trade and Development, *E-Commerce and Development Report 2002*, p43
- [86]. Zhou lin, *China Court Cases on Intellectual Property Rights*, Publisher, Kluwer Law International B.V., 2011, p 323.
- [87]. EC-Council, *Computer Forensics: Investigating Network Intrusions and Cyber Crime*, Publisher Cengage Learning, 2009, p 9-4.
- [88]. United States Code, 2006, V. 8, Title 15, Commerce and Trade, Sections 80a-1 to End, p596.
- [89]. Congressional Record, V. 145, Pt. 21, November 17, 1999 to December 3, 1999, Publisher Government Printing Office, p30501.
- [90]. Rachel Gader-Shafran, MA, jd, llm, *the trademark law dictionary*, Publisher iUniverse, 2013, p218.
- [91]. Carol Chadirjian, *The Business of Trademarks: A Practical Guide to Trademark Management for Attorneys and Paralegals*, Publisher Universal-Publishers, 2018, p134.
- [92]. Thomas Hoeren, Jochen Stauder, *International Sources of Electronic Commerce Regulation*, Publisher Lit, 2001, p281.
- [93]. United States Code Service - Volume 15 Publisher LexisNexis, Page 5
- [94]. Lanham act at 15 U.S.C. § 1117(d)
- [95]. Roman L. Weil, Peter B. Frank, Michael J. Wagner, *Litigation Services Handbook: The Role of the Financial Expert*, Publisher John Wiley & Sons, 2002, p21-10.
- [96]. Jeffery Handelman, *Guide to TTAB Practice*, Publisher Aspen Publishers Online, 2007, p A-44.
- [97]. Mark A. Glick, Lara A. Reymann, Richard Hoffman, *Intellectual Property Damages: Guidelines and Analysis*, Publisher John Wiley & Sons, 2002, p457.
- [98]. Balotti, Jesse A. Finkelstein, *The Delaware Law of Corporations & Business Organizations Statutory Deskbook*, Asben Publisher 3
- [99]. rd edition 2011, p80`.
- [100]. Reverse Domain Name Hijacking Information, on <https://www.rdnh.com/rdnh-provision-udrp/>
- [101]. Travis Crabtree, City of Paris ordered to pay for reverse domain name hijacking in groundbreaking decision, on web cite
- [102]. <https://www.emedialaw.com/city-of-paris-ordered-to-pay-for-reverse-domain-name-hijacking-in-groundbreaking-decision/>
- [103]. ADR Report - Volume 4, Publisher Pike & Fischer, 2001Page 34
- [104]. James Van Roekel, MaryAnn Bell, Bobby Ezell, *Cybersins and Digital Good Deeds: A Book About Technology and Ethics*, CRC Press, 2006, p51.