

***The Conflicts between trademark and domain
names in Arab countries – a comparative study
with the UK***

PREPARED BY ZIAD MARAQA

ZMARAQA@TAGI.COM

TABLE OF CONTENTS

INTRODUCTION.....	4
BACKGROUND.....	4
SHOULD CYBERSQUATTING BE TOLERATED.....	6
CASES.....	6
THE REGULATION OF CYBERSQUATTING.....	9
TRADEMARK DILUTION SUITS.....	9
 DOMAIN DISPUTE LAWS AND CASES IN THE EUROPEAN UNION.....	9
POLICY STATEMENT.....	11
E- TRANSACTION LAWS IN JORDAN AND U.A.E.....	13
CONCLUSION.....	15
BIBLIOGRAPHY.....	17

Cybersquatting is viewed by some as illustrating the ineffectiveness of traditional legal rules in the 'Wild Wild Web'. To what extent do you think cybersquatting should be tolerated, and how effective do you think the current system is in regulating cybersquatting?

Introduction

Domain names have sparked huge controversy in the legal system, which comes as evidence that 'the growth of the Internet has outpaced traditional legal doctrine'.¹ An attempt to register a domain name that has been previously registered by another is prevented, due to the prior registration of that domain name by the first user.² This means that two website owners cannot use the same domain names. Although two non-competing users of a trademark can legally register the same mark, they cannot identify their sites with an identical incorporation of the mark into a domain name. This leads to confusion for customers accessing both websites even if the two companies used similar domain names. As a consequence, conflict arises between companies claiming sovereignty on a borderless Internet.

A race between companies to register a domain name has sparked competition, as the 'personal' aspects of trademark use on the Internet have led companies to adopt strategies to get the most value from their trademarks. This paper will attempt to address to what extent cybersquatting should be tolerated within the legal system, and how effective the current system is in regulating cybersquatting.

Background

Cybersquatting is known as the practice of purposely registering the domain name that is the trademark of another. This does not include the registration of a domain name that is later purchased. A cybersquatter takes the domain name and tries to extract money from the trademark owner who has not registered the name.³

By registering a number of domain names, cybersquatters aim to sell the domain names at huge prices to others who may want the URL or who are prepared to pay in order to avoid confusion. This act was previously known as *information highway robbery*.⁴ Cybersquatters have also been known as *cyberpirates*. Cyberpirates benefit by either confusing customers as to the source of the goods or services sold or by generating advertising revenue from drawing additional customers.⁵

¹ S. Davidson & N. Engisch, *Trademark Misuse in Domain Name Disputes*, 13 COMPUTER LAWYER 13 Aug. 1996, 90, <http://vjolt.student.virginia.edu/graphics/vol14/v4i2a8-tucker.html#ff204> accessed on 22 July 2003.

² *Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227 (N.D. Ill. 1996).

³ Maine & Asmus, *Webiquette, Netiquette, and Cyberetiquette*, Maine & Asmus Intellectual Property, <http://www.maineandasmus.com/webiquet.htm>, accessed on 22 July 2003.

⁴ E. Swetsky, *Cybersquatting*, Lead Newsletter Article, February 1998, <http://www.advertisinglawyer.ca/news-1999-02.htm>, accessed on 22 July 2003.

⁵ K. Blackman, *The Uniform Domain Name Dispute Resolution Policy: A Cheaper Way to Hijack Domain Names and Suppress Critics*, Harvard Journal of Law & Technology, Harvard Law School, Fall, 2001, 15 Harv. J. Law & Tec 211.

As long as cybersquatters own the domain name, trademark owners cannot register their own trademark as a domain name, thus violating the fundamental rights of trademark owners to use their trademark. However, it is vital to note that the practice of reserving a domain name is not an illegal matter. It is common that cybersquatters register words that would be sought after by potential companies in the future. A trademark is therefore not breached by a domain name unless the trademark existed at the time of domain name registration. John Mercer highlights *innocent cybersquatting* which relates to cybersquatters who have no intention of harming a trademark owner, whereby the registrant uses the same trademark as another commercial entity, but not within a competing industry.⁶

On the other hand, 'the harmful kind of cybersquatting involves intentional bad faith trafficking in domain names that are the same as, or a dilution of, existing trademarks. Such domain name registrants are considered 'modern day extortion[ists]'.⁷ Mercer states that 'an illegal cybersquatter should be one who acquires a domain name for the sole purpose of obtaining money or other advantage from the trademark owner, with no intent or desire to use the domain name, except as an instrument toward this purpose'.⁸

So although many entrepreneurs are legitimately registering new trademarks as domain names for their companies, others are registering trademarks that have previously been established out of goodwill. The issue therefore is how can a legitimate domain name registrant be distinguished from one who registers a domain name in bad faith.⁹

⁶ M. Kilian, *Cybersquatting and Trademark Infringement*, E Law - Murdoch University Electronic Journal of Law, Vol 7, No 3, September 2000, <http://www.murdoch.edu.au/elaw/issues/v7n3/kilian73.html>, accessed on 22 July 2003.

⁷ C. Perry, *Trademarks as Commodities: The 'Famous' Roadblock to Applying Trademark Dilution Law in Cyberspace*, Connecticut Law Review, 32, 2000, 1127.

⁸ M Kilian, *op. cit.*

⁹ P. Boyd, *ICANN's Uniform Dispute Resolution Policy: Promoting the UDRP's good points and spanking its faults like a bad monkey*, May 2000, <http://www.techlawonline.com/articles/icann.htm>, accessed on 22 July 2003.

Should Cybersquatting be Tolerated

It is obvious that cybersquatting is a serious matter that is characteristic of the rise of the Internet. Yet the question remains to what extent should cybersquatting be tolerate within the legal system. Following are cases that address this issue.

Cases

Following a Court of Appeal decision in the One in a Million case, the courts in the UK no longer tolerated Cybersquatting. The case involved the registration by the defendants of domain names with a view to selling them at a later stage. The Court of Appeal held that the registration of domain names amounted to false representations that the defendants were associated with the brand owners, on the basis that anyone conducting a search of, for example, Marks & Spencer.co.uk would discover that the registrant is One in a Million Limited. Due to the fact that people would conclude that this company was associated with Marks & Spencer plc, this would amount to passing off. The owners relied on section 10(3) of the TMA. The defendant argued that there was no use of the mark and therefore no possibility of confusion. Nevertheless, the appeal judges held that the domain names took advantage of the distinctive character in the mark and that such use was unfair and detrimental.¹⁰

The cases *Panavision Intl v Toeppen* 141 F.3d 1316 (9th Cir. 1998) and *Intermatic, Inc v Toeppen* 947 F. Supp. 1227 (N.D. Ill. 1996) are considered the main cybersquatting cases that have had a strong impact on the development of cybersquatting case law.¹¹ A well-known cybersquatter is Dennis Toeppen who registered a host of well-known trademarks as domain names. Toeppen was sued by the trademark owners and could not however defend his rights, Panavision is one of these trademark owners.

Toeppen registered the domain name www.panavision.com and offered to sell the domain name to Panavision for \$13,000. Panavision refused the offer and brought an action under the Federal Trademark Dilution Act (FTDA). The FTDA asked the plaintiff to prove.¹²

¹⁰ N. Buke, Seminar 4 – Question 5,

<http://www.juridicum.su.se/english/master/ipl/Summaries%20Trademark%20Law/koraybukeQ5.doc>, accessed on 22 July 2003.

¹¹ C. Rains, *A Domain By Any Other Name: Forging International Solutions For the Governance of Internet Domain Names*, 14 Emory International Law Review, 355, quoted in M. Kilian, *Cybersquatting and Trademark Infringement*, E Law - Murdoch University Electronic Journal of Law, Vol 7, No 3, September 2000, <http://www.murdoch.edu.au/elaw/issues/v7n3/kilian73.html>, accessed on 22 July 2003.

¹² J. Mishkin, *Master of Your Domain - An Overview Of the Anticybersquatting Consumer Protection Act*, 2000, 18 Communications Lawyer, 3, quoted in M. Kilian, *Cybersquatting and Trademark Infringement*, E Law - Murdoch University Electronic Journal of Law, Vol 7, No 3, September 2000, <http://www.murdoch.edu.au/elaw/issues/v7n3/kilian73.html>, accessed on 22 July 2003.

- that the trademark in question is famous;
- that the defendant was using the mark in commerce;
- that the mark became famous before the defendant started using it;
- that the defendant's use of the mark dilutes the quality of the mark by diminishing the capacity of the mark to identify and distinguish goods and services.

Toeppen argued that he was not making commercial use of the name. The court, however, decided that by having offered the domain name for sale, Toeppen obviously had the intention to use the mark in commerce. The court also highlighted that a domain name carried the reputation of a trademark.

In the *Intermatic* case, the court considered Toeppen as not using the trademark in commerce due to the fact that he had merely registered it, but found infringement through dilution. The court in *Intermatic* recognised that if Toeppen were allowed to operate the web site *intermatic.com*, *Intermatic's* name and reputation would be under Toeppen.

The rulings in *Panavision* and *Intermatic* confirm that 'it is not only the unadulterated trademark that can be protected, but also any variation of it that is likely to confuse or deceive, or in some way dilute the 'distinctive quality' of the mark'.¹³ The Anticybersquatting Consumer Protection Act incorporates the dilution provisions of the FTDA, but without the FTDA's requirement for use in commerce, which leads to the broadening of the concept of trademark infringement.

One of the more recent cybersquatting cases is *Toys 'R' Us, Inc. v. Abir*. No. 97.CIV.8673, 1997 U.S. Dist. LEXIS 22431 (S.D.N.Y. Dec. 19, 1997). In this case, the defendant discovered that the domain name *toysareus.com* was not registered by the toy retailer.¹⁴ The defendant wrote to Toys 'R' Us, claiming that they had to register the name and informed them that he had himself registered it. He then offered to sell the domain name to Toys 'R' Us. When his demands were rebuffed, he wrote to Toys 'R' Us again threatening to establish a competing toy company that would sell its products using the website *www.toysareus.com*. He made this demand despite the fact that the defendant admitted to intentionally copying the plaintiff's trademark when he registered the *toysareus.com* domain name.

Toys 'R' Us sued the defendant for trademark infringement (Section 32(1) of the Lanham Act), false designation of origin (Section 43(a) of the Lanham Act), and trademark dilution (Section 43(c) of the Lanham Act). In addition,

¹³ C. Rains, *A Domain By Any Other Name: Forging International Solutions For the Governance of Internet Domain Names*, 14 *Emory International Law Review*, 367, quoted in M. Kilian, *Cybersquatting and Trademark Infringement*, *E Law - Murdoch University Electronic Journal of Law*, Vol 7, No 3, September 2000, <http://www.murdoch.edu.au/elaw/issues/v7n3/kilian73.html>, accessed on 22 July 2003.

¹⁴ R. Tucker, *Information Superhighway Robbery: The Tortious Misuse of Links, Frames, Metatags, and Domain Names*, *Virginia Journal of Law and Technology*, University of Virginia, Fall 1999, 4 VA. J.L. & TECH. 8, <http://vjolt.student.virginia.edu/graphics/vol4/v4i2a8-tucker.html#ff241>, accessed on 22 July 2003.

Toys 'R' Us brought common law claims for violation of New York's unfair competition law.

In granting the requested injunctive relief, the court first found that an injunction was appropriate because the plaintiff had established a likelihood of success on the trademark infringement count. Toys 'R' Us proved to the court's that it had a valid mark subject to protection, and that the defendant's mark resulted in a likelihood of confusion. Therefore, likelihood of confusion was presumed as a matter of law because the defendant admitted that he intentionally copied the plaintiff's trademark. The court also found that the plaintiff established a likelihood of success on their dilution claims because it established that the "R' Us" marks are famous, and that the defendant's use of those marks in a commercial manner diluted those marks. Since those were the only two elements that must be established to prove a claim under the Federal Trademark Dilution Act, Toys 'R' Us was entitled to injunctive relief.¹⁵

¹⁵ R. Tucker, *Information Superhighway Robbery: The Tortious Misuse of Links, Frames, Metatags, and Domain Names*, Virginia Journal of Law and Technology, University of Virginia, Fall 1999, 4 VA. J.L. & TECH. 8, <http://vjolt.student.virginia.edu/graphics/vol4/v4i2a8-tucker.html#ff241>, accessed on 22 July 2003.

The Regulation of Cybersquatting

Trademark Dilution suits¹⁶

The Federal Trademark Dilution Act of 1995 protects trademarks, codified in the Lanham Act, that states that the plaintiff must prove that: (1) their mark is famous; (2) there is commercial use of the mark by another party in commerce; and (3) such commercial use causes dilution of the distinctive quality of the mark. Like trademark infringement, dilution requires that a mark be used in commerce. However, unlike infringement, dilution protection also extends to unregistered marks.

To win a trademark action and receive an injunction, the plaintiff must prove dilution. Traditionally, the dilution doctrine protects a mark from either blurring of the distinctive quality of the mark or the tarnishing of the mark through negative associations created by a defendants use. In the first instance, dilution by blurring occurs whenever a junior mark is either identical to or sufficiently similar to the famous mark that persons viewing the two marks will instinctively make a mental association between the two. The second traditional means of dilution is tarnishment, which could arise when the goodwill and reputation of a plaintiff's trademark is linked to products that are of poor quality. In the domain name world, trademark dilution occurs when a cybersquatter uses the domain name to divert traffic, confuse the viewer as to ownership of goods, or tarnish the goods of the legitimate trademark owner.

At present, a trademark dilution action is effective at combating the use of a similar domain name that is tarnishing a famous mark. Nevertheless, its remedies and the cost of litigating in federal court limit its use. In addition, a dilution action cannot gain any remedy outside of injunctive relief, like the transfer of the domain name, unless the plaintiff can show wilful intention to cause dilution. To fight this phenomenon, Congress enacted the Anti-Cybersquatting Protection Act that allow statutory damages.

Domain Dispute Laws and Cases in the European Union¹⁷

Due to the lack of dispute resolution policies throughout the EU, the WIPO held a conference in February 2001 where it issued the 'WIPO ccTLD Best

¹⁶ P. Boyd, *ICANN's Uniform Dispute Resolution Policy: Promoting the UDRP's good points and spanking its faults like a bad monkey*, May 2000, <http://www.techlawonline.com/articles/icann.htm>, accessed on 22 July 2003.

¹⁷ *Domain Dispute Laws and Cases in the European Union*, <http://www.juridicum.su.se/english/master/ip1/Summaries%20Trademark%20Law/koraybukeQ5.doc>, accessed on 20 July 2003.

Practices for the Prevention and Resolution of Intellectual Property Disputes'. In this report, WIPO called for ccTLD administrators to require better identification of companies and individuals that register domain names and mandatory dispute resolution procedures. WIPO urged domain registries to adopt a dispute resolution policy similar to the UDRP. It is expected, though, that if WIPO's recommendations are implemented, it could be a long time before the EU has a unified dispute resolution policy.

Since most registries throughout the EU do not offer a dispute resolution process, a party must seek relief in court to protect its rights against cybersquatters. Similar to the United States, courts in Europe have a range of different laws that they can apply to domain disputes, such as trademark laws. Trademark law is typically the most uniform throughout the EU, especially with the implementation of Council Directive 89/104/EEC, which has coordinated the definition of trademarks and defined infringement situations.

Courts throughout Europe have typically found that the use of a domain name that is identical or similar to a trademark constitutes trademark infringement if used in bad faith or in connection with the sale of competing products or services and will permit the trademark holder to obtain injunctive relief.

European courts do not agree on whether the act of registering a domain name without having an active web site or offering the domain for sale constitutes trademark infringement. Relevant cases include *British Telecommunications plc. v. One In A Million Ltd.*, where the British Court of Appeal found that the act of registering known names and trademarks constituted grounds for trademark infringement, even though the domains were inactive and the registrant did not offer to sell the domain names.

Therefore, in the UK, the owner of a famous mark can take action against a cybersquatter as soon as it knows that the registration of an infringing domain has taken place. Italy has also extended such rights to situations where a name has a reputation in Italy, allowing the owner of a famous mark to obtain an infringement ruling against a party attempting to register a domain name. On the other hand, in the Danish 'Beologic' case, the Municipal Court of Copenhagen found that the mere registration of domain names or the offer to resell them did not violate trademark law, since the defendant was not conducting business under the marks. The court did find, though, that the defendant violated the Marketing Act, which forbids "unfair marketing" and common law conversion.

Some countries have enacted or are in the process of enacting new legislation to deal with cybersquatting issues. In April 2001, the Italian government responded to the cybersquatting phenomenon with Bill No. 4564 on 'Use of names for identification of domain names and network services'. The bill provides rules for using domain names and prohibits the registration of domain names corresponding to names, trade names, or trademarks already in use by third parties due to potential confusion of the general public.

In cases of infringement, the domain name is cancelled, and damages can be awarded to the plaintiff.¹⁸

Policy statement ¹⁹

The International Chamber of Commerce (ICC) considers that domain name applicants should provide the same level of information as would be required for a trade mark application and that this information should be publicly available on the same basis. There should also be provision for sanctions for use of false address details and presumptions about service of correspondence sent by registered mail to the specified address. There is some support within ICC for the domain name agreement to require a street address for the applicant rather than accepting a post office box, as ICC members have found a significant correlation among cybersquatting and fraud from applicants who list fraudulent post office addresses. A physical street address would enable intellectual property owners to more easily contact and locate the registrant in the event of a domain name dispute. Similar to the NSI WHOIS database in existence today, the applicant should also provide an administrative and engineering contact who can also be qualified to accept service of process.²⁰

Intellectual property rights holders frequently rely on databases, like the WHOIS database, to find user names, addresses, and evidence of cybersquatting. Easy and quick access to databases is needed to ascertain the true identity and addresses of fraudsters, cybersquatters and domain name infringers. Even with open access to WHOIS, ICC members experience difficulties with fraudulent information in the databases.²¹

A statement in the registration agreement concerning an intention to use a domain name and the intended purpose would be a helpful mechanism for discouraging cybersquatting, fraud and other illegitimate uses of domain names. ICC believes however that the issue of the intended purpose use of the domain name could be dealt with more effectively by having (g)TLDs assigned to specific fields of use (e.g. airline, bank, cars etc) with provision for cancellation on challenge if the domain name was not used for the specified field of business. It could also be useful to include a requirement that use of

¹⁸ K. Buke, *Seminar 4 – Question 5 N*,

<http://www.juridicum.su.se/english/master/ipl/Summaries%20Trademark%20Law/koraybukeQ5.doc>, accessed on 22 July 2003.

¹⁹ *Commission on Intellectual and Industrial Property*, 18 March 1999,

http://www.iccwbo.org/home/statements_rules/statements/1999/wipo_interim_report_RFC-3.asp, accessed 20 July 2003.

²⁰ *ICC The world business organization*, 50

http://www.iccwbo.org/home/statements_rules/statements/1999/wipo_interim_report_RFC-3.asp, accessed on 22 July 2003.

²¹ *ICC The world business organization*, 51

http://www.iccwbo.org/home/statements_rules/statements/1999/wipo_interim_report_RFC-3.asp, accessed on 22 July 2003.

the domain name has to be made within a certain time after registration, say one year. "Use" for the purpose of this requirement should also be clarified²²
ICAAN Dispute Resolution Procedure:²³

The trend to protect legitimate users has been reflected in the fact that NSI is no longer implementing its own very trademark-owner-friendly dispute resolution policy, but has adopted the Uniform Domain Name Dispute Resolution Procedure settled by ICANN. Key features are:

- Right to transfer of name (no damages) where
- The domain name is identical or confusingly similar to a mark in which the complainant has rights; AND
- The domain name registrant has no rights or legitimate interests in respect of the domain name; AND
- The domain name has been registered and is being used in bad faith.

N.B. all three elements must be proved.

Factors which will be taken into account when considering bad faith:

- Intent to profit through domain speculation
- Intent to prevent the owner of a trademark having the corresponding domain name where a history of such practices is shown
- Intent to disrupt another's business
- Intent to pass off

Factors which may be considered as to legitimacy of registration

- Bona fide use before notification of dispute
- Bona fide use of own name
- Non commercial or fair use without intent to pass off or tarnish another's reputation or mark

Once a decision by the panel has been made it will not be implemented for ten days during which time either party may apply to a national Court. Whilst people may still argue that the trademark owner with money still has the advantage, the new policy is a lot fairer than the old NSI policy and the advantage given to those with money is no more than in any other field of litigation. The policy was first used successfully by the World Wrestling Federation who reclaimed worldwrestlingfederation.com using the procedure. The registrant's offer to sell the name to the Federation was taken to be evidence of bad faith. Since then at least half a dozen applications by trademark owners have been successful.

However, it can easily be seen that the 'hatfield.com' case of bona fide use of own surname and cases of legitimate use in different fields such as 'clue.com' and 'avnet.co.uk' would now be decided in the same way under the dispute resolution policy as through the Courts.

²²ICC *The world business organization*, 62, http://www.iccwbo.org/home/statements_rules/statements/1999/wipo_interim_report_RFC-3.asp, accessed on 22 July 2003.

²³ D. Osborne, *Domainname Notes*, http://www.domainnotes.com/news/print/0,,5281_350381,00.html, accessed on 22 July 2003.

e- Transaction laws in Jordan and U.A.E

UAE (Dubai) Electronic Transactions and Commerce Law

Dubai Electronic Transactions and Commerce Law No.2/2002 is applied in the Emirate of Dubai only. There is a federal draft law under preparation to be applied all over the UAE. The law consists of 5 chapters, 39 articles addressing different issues such as definitions; electronic transactions, records and electronic signature requirements; as well as the conditions related to the certificates, authentication, interpretation of the law, application, and the acceptance of the electronic transaction.

Electronic Authentication Parties

The UAE electronic transactions and commerce law delegated the electronic authentication to the "Authentication Services Controller" who is appointed by the Chairman of Dubai Technology and Media Free Zone Authority where article 24 of the law stipulates that the supplier of the certification services shall provide reasonably accessible means which enable a Relying Party to ascertain the identity of the Supplier of Certification Services; the site control over the signature tool, that the person who is identified in the Certificate had control over the Signature Device referred to in the Certificate; the method used to identify the Signatory; any limitations on the purposes or value for which the Signature Device may be used; whether the Signature Device is valid and has not been compromised; whether means exist for the Signatory to give notice; and ascertain the identity of the contracting parties as article 24 of the electronic transactions law provides for the requirements to be met in the information certificate.

Jordan Electronic Transactions Law

Passing the electronic transactions interim law No. 85 of 2001 was passed in Jordan is considered a step to launch the electronic commerce and e-government project. Jordan electronic transactions interim law came into force in April 2002. It consists of many articles covering all legislative and legal issues in the internet field. The law aims to establish a legal framework and electronic transactions regulations to simplify conduct the transactions, contracts and agreements electronically, and to eliminate the barriers before the e-commerce.

The law consists of 41 articles and addresses different issues, including the general provisions, records, contracts, messages, and e-signatures, transferable electronic note, electronic transfer of funds, securing the electronic records and electronic signature, penalties, and final provisions.

Articles 7, 8, and 9 of the Jordan electronic transactions law came in substantial provisions that legally recognize the electronic means and that the electronic records, contracts, messages, and signatures shall be deemed to produce the same legal effect as written documents, instruments and

signatures pursuant to the provisions of legislation in force and with respect to enforceability and admissibility as evidence.

Notes on the Jordan and UAE electronic commerce law:

1. UAE and Jordan experience in enacting such laws is still brief, and none of the issues addressed by such law are applied before the courts, though it is hoped to be the case in the future.
2. Many other issues on electronic commerce have been overlooked by these laws. Thus, UAE and Jordan alike don't have that big experience in the enactment of laws regulating e-commerce, IT, and Internet.
3. There are some commonalities between UAE and Jordan laws either in articles, provisions, subjects, or terms among other things. This is not strange as most Arab laws derive their provisions from the same source, namely; UNCITRAL Model Law on Electronic Commerce for 1996, and UNICITRAL Model Law on Electronic Signatures for 2001.
4. Unlike the expectations, UAE and Jordan have not enacted regulations or bylaws to enforce the electronic transactions and dealings laws to regulate electronic authentication parties. This is one negative area that must be taken into consideration because the absence of regulations and bylaws to enforce the e-transactions and detail laws on technical issues makes such laws mere ink on paper. This is inconsistent with the universal trend in enacting laws that give the general guide lines and leave the narrow details to be handled by regulations and bylaws.
5. Understanding technology and technical issues is undoubtedly vital when drafting e-commerce laws. It can safely be said that most Arab laws are weak in this area, mainly because the technical issues legislators lack knowledge on technical issues which consequently lead to the introduction of unclear ambiguous articles causing some confusion for the users of these laws.
6. UAE and Jordan, which enacted laws on electronic transactions and signatures, did not conduct a critical comprehensive review of their applied laws such as evidence, penalty, and commercial laws, while these laws are well related to the electronic transactions and signatures laws and should be examined in terms of consistence with the electronic transactions and commerce laws. This insufficient review may lead to the enactment and introduction of contradictory laws and articles. Although most transactions laws stipulate that the new laws shall prevail over the previous ones in case of such contradiction, the older provisions and laws should be considered when enacting the new ones.
7. Development of electronic commerce and information technology in any country is not restricted to the enactment of e-commerce only. It is only after a package of areas including awareness for example is developed, that laws can play their role in regulating the relations arising from the use of the internet. Hence, this policy must be applied by the government.

Conclusion

Based on the foregoing, and after three years of passing and enforcing Jordan and UAE law, launch of organizations and associations specialized in the Cyber Law, establishment of Arab Association of Cyber Law in the International Conference of the Cyber Law which was held in Al-Ghardaqah, Egypt at the end of August 2005 where the conference recommended many important topics to be addressed in the Arab countries, an Arab regulations should be enacted in the field of Cyber Law based on the Arab Internet Document which was raised in the conference and to consider it as one of the Arab League documents, and get it ratified by the Arab governments and legislative councils to be a unified Arab law in the field of the internet.

Clearly, the establishment of an unauthorized link from one Web site to another exposes the owner of the linking site to potential tort liability any number of ways. The possible tort claims that can result from an unauthorized linking range from the obvious (copyright infringement, trademark infringement, trademark dilution, false designation of origin, and unfair competition) to the sublime (invasion of privacy, defamation, tortious interference with contract, consumer fraud, or false and deceptive trade practices).

Technology readily available to anyone capable of maintaining a Web site readily permits the blocking of an unauthorized links, redirecting such links to the desired entry point, and the disabling of any frames software used on the linking site. Under these circumstances, should a plaintiff be permitted to seek an award of substantial money damages for an injury that the plaintiff could have avoided by the minimal expenditure of time and effort before the injury occurred? No. The well-established Web culture generally implies a license to link without prior authorization. Every potential plaintiff makes a conscious decision to gain itself of the Internet knowing that unauthorized links were possible, and every potential plaintiff has the technology available to detect and prevent unauthorized links. Given these facts, this author firmly believes that the doctrine of preventable consequences could prohibit a plaintiff from claiming any injury as damage that it could have avoided through the implementation of reasonable, technologically feasible safeguards either before or after the allegedly tortious conduct.²⁴

Although some big companies are using legal threats to scare domain holders into giving up property that is legitimately theirs, there are many that are rightfully victims of cybersquatting. In conclusion, there are new laws being written up at this moment in order to combat this new practice, some controversial, and some put in place to protect cybersquatters' rights, but what

²⁴ R. Tucker, *Information Superhighway Robbery: The Tortious Misuse of Links, Frames, Metatags, and Domain Names*, Virginia Journal of Law and Technology, University of Virginia, Fall 1999, 4 VA. J.L. & TECH. 8, <http://vjolt.student.virginia.edu/graphics/vol4/v4i2a8-tucker.html#ff241>, accessed on 22 July 2003.

ever the law, buying the domain name, with the intent to sell the names for a profit, is not right and is done so in bad faith.²⁵

²⁵ Mary's Project Page, <http://www.infm.ulst.ac.uk/~esf0mom.esf0/projectpage.html>, accessed on 24 July 2003.

Bibliography

S. Davidson & N. Engisch, Trademark Misuse in Domain Name Disputes, 13 COMPUTER LAWYER 13 Aug. 1996, 90, <http://vjolt.student.virginia.edu/graphics/vol4/v4i2a8-tucker.html#ff204> accessed on 22 July 2003.

Intermatic Inc. v. Toeppen, 947 F. Supp. 1227 (N.D. Ill. 1996).

Maine & Asmus, Webiquette, Netiquette, and Cyberetiquette, Maine & Asmus Intellectual Property, <http://www.maineandasmus.com/webiquet.htm>, accessed on 22 July 2003.

E. Swetsky, Cybersquatting, Lead Newsletter Article, February 1998,

<http://www.advertisinglawyer.ca/news-1999-02.htm>, accessed on 22 July 2003.

K. Blackman, The Uniform Domain Name Dispute Resolution Policy: A Cheaper Way to Hijack Domain Names and Suppress Critics, Harvard Journal of Law & Technology, Harvard Law School, Fall, 2001, 15 Harv. J. Law & Tec 211.

M. Kilian, Cybersquatting and Trademark Infringement, E Law - Murdoch University Electronic Journal of Law, Vol 7, No 3, September 2000, <http://www.murdoch.edu.au/elaw/issues/v7n3/kilian73.html>, accessed on 22 July 2003.

C. Perry, Trademarks as Commodities: The 'Famous' Roadblock to Applying Trademark Dilution Law in Cyberspace', Connecticut Law Review, 32, 2000, 1127.

M Kilian, op. cit.

P. Boyd, ICANN's Uniform Dispute Resolution Policy: Promoting the UDRP's good points and spanking its faults like a bad monkey, May 2000, <http://www.techlawonline.com/articles/icann.htm>, accessed on 22 July 2003.

N. Buke, Seminar 4 – Question 5,

<http://www.juridicum.su.se/english/master/ipl/Summaries%20Trademark%20Law/koraybukeQ5.doc>, accessed on 22 July 2003.

C. Rains, A Domain By Any Other Name: Forging International Solutions For the Governance of Internet Domain Names, 14 Emory International Law Review, 355, quoted in M. Kilian, Cybersquatting and Trademark Infringement, E Law - Murdoch University Electronic Journal of Law, Vol 7, No 3, September 2000,

<http://www.murdoch.edu.au/elaw/issues/v7n3/kilian73.html>, accessed on 22 July 2003.

J. Mishkin, Master of Your Domain - An Overview Of the Anticybersquatting Consumer Protection Act, 2000, 18 Communications Lawyer, 3, quoted in M. Kilian, Cybersquatting and Trademark Infringement, E Law - Murdoch University Electronic

Journal of Law, Vol 7, No 3, September 2000,

<http://www.murdoch.edu.au/elaw/issues/v7n3/kilian73.html>, accessed on 22 July 2003.

C. Rains, A Domain By Any Other Name: Forging International Solutions For the Governance of Internet Domain Names, 14 Emory International Law Review, 367, quoted in M. Kilian, Cybersquatting and Trademark Infringement, E Law - Murdoch University Electronic Journal of Law, Vol 7, No 3, September 2000,

<http://www.murdoch.edu.au/elaw/issues/v7n3/kilian73.html>, accessed on 22 July 2003.

R. Tucker, Information Superhighway Robbery: The Tortious Misuse of Links, Frames, Metatags, and Domain Names, Virginia Journal of Law and Technology, University of Virginia, Fall 1999, 4 VA. J.L. & TECH. 8, <http://vjolt.student.virginia.edu/graphics/vol4/v4i2a8-tucker.html#ff241>, accessed on 22 July 2003.

R. Tucker, Information Superhighway Robbery: The Tortious Misuse of Links, Frames, Metatags, and Domain Names, Virginia Journal of Law and Technology, University of Virginia, Fall 1999, 4 VA. J.L. & TECH. 8,

<http://vjolt.student.virginia.edu/graphics/vol4/v4i2a8-tucker.html#ff241>, accessed on 22 July 2003.

P. Boyd, ICANN's Uniform Dispute Resolution Policy: Promoting the UDRP's good points and spanking its faults like a bad monkey, May 2000,

<http://www.techlawonline.com/articles/icann.htm>, accessed on 22 July 2003.

Domain Dispute Laws and Cases in the European Union, <http://www.juridicum.su.se/english/master/ipl/Summaries%20Trademark%20Law/koraybukeQ5.doc>, accessed on 20 July 2003.

K. Buke, Seminar 4 – Question 5 N, <http://www.juridicum.su.se/english/master/ipl/Summaries%20Trademark%20Law/koraybukeQ5.doc>, accessed on 22 July 2003.

P. Boyd, ICANN's Uniform Dispute Resolution Policy: Promoting the UDRP's good points and spanking its faults like a bad monkey, May 2000,

<http://www.techlawonline.com/articles/icann.htm>, accessed on 22 July 2003.

Commission on Intellectual and Industrial Property, 18 March 1999,
http://www.iccwbo.org/home/statements_rules/statements/1999/wipo_interim_report_RFC-3.asp, accessed 20 July 2003.

ICC The world business organization, 50

http://www.iccwbo.org/home/statements_rules/statements/1999/wipo_interim_report_RFC-3.asp, accessed on 22 July 2003.

ICC The world business organization, 51

http://www.iccwbo.org/home/statements_rules/statements/1999/wipo_interim_report_RFC-3.asp, accessed on 22 July 2003.

ICC The world business organization, 62,

http://www.iccwbo.org/home/statements_rules/statements/1999/wipo_interim_report_RF_C-3.asp, accessed on 22 July 2003.

D. Osborne, Domain name Notes,
http://www.domainnotes.com/news/print/0,,5281_350381,00.html, accessed on 22 July 2003.

R. Tucker, Information Superhighway Robbery: The Tortious Misuse of Links, Frames, Metatags, and Domain Names, Virginia Journal of Law and Technology, University of Virginia, Fall 1999, 4 VA. J.L. & TECH. 8,

<http://vjolt.student.virginia.edu/graphics/vol4/v4i2a8-tucker.html#ff241>, accessed on 22 July 2003.

Mary's Project age,
<http://www.infm.ulst.ac.uk/~esf0mom.esf0/projectpage.html>, accessed on 24 July 2003.