Thesis: The Role of a Domain Name Registrar as an Internet Intermediary

Hazel Murphy

ANR: 565479

LLM Law and Technology

Supervisor: M. H. M. Schellekens.

Contents

List of Abbreviations

CJEU	Court of Justice of the European Union
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
ECHR	European Convention on Human Rights
EFF	Electronic Frontier Foundation
EU	European Union
ICANN	Internet Corporation of Assigned Names and Numbers
IP	Internet Protocol
IPR	Intellectual Property Rights
ISP	Internet Service Provider
OECD	Organisation for Economic Co-operation and Development
OS	Operating System
TLD	Top Level Domain
UDRP	Uniform Domain Name Dispute Resolution Policy
UK	United Kingdom
UNESCO	United Nations Educational, Scientific and Cultural Organisation

Chapter 1 – Introduction

1.1 Background and problem description

The internet is a global network of computers operated by groups and individuals, the computers are all connected for the purpose of sharing information. The internet connects machines all over the world therefore it is multi-jurisdictional and this lack of singular control can lead to issues with governance. There are no international laws managing the use of the internet, so different countries have different regulations and online intellectual property rights infringers may use this to their advantage. The internet is subject to laws but requires more specific legislation as it is too difficult to govern with the traditional law from the offline world. There are ongoing disputes between rights holders and internet intermediaries about the liability for cases of online infringement. Currently, the law is unclear about liability for registrars and case law in the European Union is providing conflicting decisions. To begin, we will look at the opposing judicial outcomes of *KeySystems v Universal Music*[1] and the *EuroDNS*[2] case.

KeySystems[3] is a German case where the court stated that if the registrar did not remove the online fraudulent content then they would be held liable for the copyright infringement of the website users. The result was that the registrar had to restrict access to the whole website by blocking the domain name. KeySystems was the registrar for h33t.com, at the time one of the biggest BitTorrent sites on the internet. The registrar received a court injunction to remove the domain name because they did not take urgent action of a 'concrete indication' for a violation of copyright infringement. On the h33t.com website, users could download content without the permission of the copyright owner through peer-to-peer file sharing. This particular case was brought by Universal Music concerning the download of Robin Thicke's album "blurred lines". The

[1] *Universal Music v Key-Systems GmbH* [2014] Regional Court of Saarbrücken.
[2] *Association Francaise pour le Nommage Internet en Coopération*, Paris Court of Appeal, 19 October 2012.
[3] *Universal Music v Key-Systems GmbH* [2014] Regional Court of Saarbrücken.

German registrar claimed they were not responsible for the copyright infringement. The court in Saarbrücken noted that the registrar was given notice about the unlawful activities and held that if the registrar knew of a clear breach of the law then they must immediately terminate the access to the unlawful content. The registrar refused to act despite multiple requests. The action would have ended if the registrar disconnected the domain name and ensured the name would be discontinued but they were unwilling to do both as they believed they simply provided a domain name and the actions of the registrant is out of their control. KeySystems argued that the company was only providing a technical service. Universal Music's attorney argued that registrars "do whatever they want these days" instead of acting with accountability.[4] The case was appealed but dismissed and the domain name was removed. This case was the first of its kind where a registrar was held liable for the copyright infringement of a torrent site. General Counsel for the registrar, Volker Greimann, said this injunction would "constitute an undue expansion of the legal obligations of each registrar based in Germany, endangering the entire business model of registering domain names".[5]

EuroDNS[6] is a French case where the court did not hold the Luxembourg based domain name registrar, EuroDNS, liable for trademark infringing domain names registered by thirteen French companies. It was argued that the registrar neglected to monitor the registration of domain names and failed to block the name after receiving knowledge of the infringement. The court noted that the registrar was exempt from liability the same way Internet Service Providers (ISPs) could be under the E-Commerce Directive. EuroDNS stated that a registrar's role had a "strict technical nature following specific requests from customers who bear the sole responsibility of

[4] 'German Court Says Domain Registrar Can Be Held Liable for the Infringement of Their Customers' (*The Domains*, 2014) <http://www.thedomains.com/2014/11/07/german-court-says-domain-registrar-can-be-held-liable-for-the-infringement-of-their-customers/> accessed 30 June 2016.

[5] 'German Court Blurs Lines of Registrar Responsibility' (*Internet Commerce Association*, 2014) <http://www.internetcommerce.org/blurred_lines/> accessed 6 August 2016.

[6] Association Francaise pour le Nommage Internet en Coopération Paris Court of Appeal, 19 October 2012.

choosing and using the domain name".[7] The Court held that registrars were not required to carefully screen for all well-known trademarks. The Appeals court also believed that such a responsibility would cause an unfair financial and technical burden. It was noted that if they were obliged to implement these additional measures, the registrar would be deciding on an issue that was beyond their skillset, as they are not intellectual property lawyers. In addition to this, the appeals court held that a request to block the domain names was not enough for them to act and they would require a court order.

The conflicting decisions show a lack of clarity and harmonisation in EU law. While one case was dealing with copyright law and the other with trademark law, they both concerned the level of engagement required by the registrar. The support for the involvement of internet intermediaries is growing.[8] Schellekens notes in his article 'Liability of Internet Intermediaries: A Slippery Slope?'[9], if internet intermediaries begin to take responsibility to prevent illegal and harmful content then the duty of care will increase and it may be hard to identify a cut-off point. This is interesting to consider because if registrars begin to take down domain names upon notification from a third party then it opens up floodgates of similar notices and soon it may reach a point where they become strictly liable. Registrars are providing a critical infrastructure and should not be deterred from providing this service. Registrars are not lawyers and there is a chance, especially in more complex cases, that they will make an erroneous judgement about an infringement. It is believed that the role of the registrar is purely technical and they cannot be responsible for ensuring that the domain names which are registered are not infringing trademarks or that the content is not unlawful.

---

[7] Domain-Name Registrars Exempt From Trademark Liability' (*Intellectual Property Watch*, 2009) <http://www.ip-watch.org/2009/09/17/france-domain-name-registrars-exempt-from-trademark-liability/.> accessed 1 August 2016.

[8] Organisation for Economic Co-operation and Development, 'Communiqué On Principles For Internet Policy-Making' (2011) <http://www.oecd.org/internet/innovation/48289796.pdf> accessed 6 August 2016.

[9] Maurice Schellekens, 'Liability of Internet Intermediaries: A Slippery Slope?' (2011) 8 SCRIPTed <http://www2.law.ed.ac.uk/ahrc/script-ed/vol8-2/schellekens.pdf> accessed 23 June. 2016.

1.2 Significance

There are close to 300 million registered domain names in the world.[10] Domain names can be quickly and easily registered at a low cost from a domain name registrar. Difficulties can arise when there are cases of infringement with the domain name itself or if there is unlawful content on the website, because of this there is unwelcomed, increased pressure on domain name registrars to use their power to block domain names. If the domain name is unavailable, while not impossible to reach, the content becomes difficult to access unless the user is technologically skilled. Domain names are seen as an online identity and this is what makes them so valuable. They make it much simpler for internet users to remember website addresses. These addresses are known as Internet Protocol (IP) addresses and a system called the Domain Name System (DNS) translates the domain name into the numerical IP address for the Operating System (OS) to understand.

In the EU, the lack of clear guidelines for blocking domain names has created some uncertainty in the industry. With the E-Commerce Directive, registrars cannot be held liable for assisting infringement until they have knowledge, only then they are no longer protected under the Directive. However, it lacks clarity and there are unanswered questions, such as in what kind of manner must they receive this information so it is known that they were appropriately aware and when do they become liable after obtaining knowledge. The domain name registration market has become highly competitive and impose an overly burdensome obligation on registrars which may deter them from carrying out this vital contribution to the internet, therefore lowering competition and increasing prices. It impacts a number of fundamental human rights including freedom of speech and freedom to conduct business. This is why the *KeySystems*[11] judgement

[10] 'Internet Grows to 296 Million Domain Names in the Second Quarter Of 2015' (*VeriSign*, 2015) <https://www.verisign.com/en_US/internet-technology-news/verisign-press-releases/articles/index.xhtml?artLink=aHR0cDovL3ZlcmlzaWduLm13bmV3c3Jvb20uY29tL2FydGljbGUvcnNzP2lkPTE5ODUwMzk%3D> accessed 28 June 2016.

[11] *Universal Music v Key-Systems GmbH* [2014] Regional Court of Saarbrücken.

is so important. It is the first of its kind where the domain name registrar was held liable for the actions of the website users because they had received notice to take down the domain name and refused to do so and were thus issued with a court injunction. It is a worrying decision because it could open floodgates for more cases similar to this. The registrar was so far removed from the conduct yet they were still liable for the actions of the users of a torrent website. Even though the website just hosted the torrent tracker therefore there was no actual infringing content on the website and a user used the tracker to download files of a music album.

1.3 Research Question

What responsibilities should rest on a domain name registrar as an internet intermediary where it concerns illegal content on a website accessible through domain names in their registration?

- What protection is afforded to the registrar under EU law?
- When are registrars obliged to act with due consideration for freedom of expression, freedom to conduct business, effectiveness of a possible measure and proportionality?

1.4 Methodology and Structure

This thesis will consider the role of domain name registrars acting as internet intermediaries, it looks at what protection they have and when are they obliged to act. The main focus will be on copyright infringement as it is a prominent issue in today's society. Chapter one is an introduction to domain names and the basis for this thesis is explained. Chapter two gives a description of important terms that are relevant for the understanding of the rest of the paper, these are the Domain Name System (DNS), the Internet Corporation of Assigned Names and Numbers (ICANN), the Uniform Domain Name Dispute Resolution Policy (UDRP). It examines the role of internet intermediaries with an emphasis on domain name registrars and Internet Service Providers (ISPs) because in the past decade there has been a demand on ISPs to stop online

infringement but now this burden is also shifting to domain name registrars.[12] The registrars are the new entities that companies are opting to try and hold liable for online issues. Chapter three will examine a typical contract between a registrar and a registrant, they are usually a standard contract as ICANN requires certain policies to be implemented into all ICANN accredited registrars agreements. This chapter will also include an analysis of the applicable law to domain name registrars. The registrar's rights and responsibilities are primarily laid out in the E-Commerce Directive, the Enforcement Directive, the Copyright in the Information Society Directive and other EU law. Chapter four examines the fundamental rights in the EU, namely the freedom to conduct business and freedom of information. This chapter looks at how to justify blocking a domain name before implementation. It examines balancing, effectiveness and proportionality. Chapter five is a conclusion where all relevant information is brought together in an attempt to clarify the role of domain name registrars acting as internet intermediaries.

[12] *Belgian Society of Authors, Composers, and Publishers (SABAM) v SA Tiscali (Scarlet)* [2007] District Court of Brussels No. 04/8975/A – Court ordered the ISP to filter illegal content. This was the first of its kind in Europe.

Chapter 2 – Explanations

2.1 Introduction

A domain name is used to access a website. The internet is authoritatively made up of IP addresses and not names, therefore every web server requires a domain name system server to translate domain names into these addresses. The domain name system (DNS) is a crucial part of the internet and accounts for its dominance in the world today as users can easily access websites. It represent an Internet Protocol (IP) address in a simple way, with words rather than numbers. Having names makes the addresses effortless for people to remember. Domain names are all unique and are obtained on a first come-first served basis from ICANN, through a certified registrar. ICANN is the organisation responsible for the maintenance relating to the namespaces of the internet. It gives the job of domain name registration to ICANN accredited registrars. There are almost one thousand domain name registrars globally[13], before the introduction of ICANN in 1998, Network Solutions had a monopoly over this industry.[14] Now all this competition has lowered the price of acquiring a domain name. Each registrar has their own terms and conditions which must be accepted when purchasing a domain name, they are usually all quite similar and closely related to ICANNs model policy and procedure as ICANN has a minimum standard practice.[15] This chapter gives an explanation of terms to help the reader get a better understanding for the thesis.

[13] 'Accredited Registrars' (*ICANN*) <https://www.icann.org/registrar-reports/accredited-list.html> accessed 6 August 2016.
[14] 'Network Solutions 30 Years of Experience' (*Network Solutions*) <http://www.networksolutions.com/why-choose-netsol/company-history.jsp> accessed 2 July 2016.
[15] 'Registrar Accreditation Agreement' (*Icann.org*, 2013) <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en> accessed 27 June 2016.

2.2 Domain Name System

Computers are connected by a large network. Each of these computers can be identified by a string of numbers know as an internet protocol (IP) number. The domain name system converts domain names into these numbers and saves all the conversion information in distributed databases. The DNS system was created out of convenience for its users. It allows names to be given to IP numbers as it is challenging to remember large numerical series. The IPv4 numbers are difficult to remember (eg. 12.68.89.419) but even more difficult is the new IPv6, which is made up for 8 number blocks (eg. 2003:2201:4339:0000:0000:0000:4193:1234). It is a hierarchically designed system, working right to left.

For example, on an internet browser, a user enters in the domain name www.tilburguniversity.edu. When a user types in a domain name address into the browser, the browser and operating system (OS) will first determine whether the computer knows what the IP address is for this domain name. It could be saved on the computer memory in the cache. A computer cache is where data which has been previously used is stored temporarily in order to speed up future data requests. If the OS does not know the IP address, it will send a request to a resolving name server. A resolving name server is usually provided by the Internet service provider and these resolving name servers discover information about the other servers. The OS queries the name server for the domain name. If the resolving name server does not have the name saved in its cache memory then it will direct the query to the correct root name server. The root name server contains IP addresses of TLD registries and directs requests to the correct TLD name server. Therefore, if the root name server does not have the address, it will direct the query to the '.edu' TLD name server. When it reaches the TLD name server and the address is not at this server, it will direct the query to the 'tilburguniversity.edu' name server, which are known as the authoritative name servers. When a domain name is bought, the domain name registrar informs the registry which authoritative name servers that domain name should use. The

authoritative name servers will have the address. The resolving name server gets the required information from the authoritative name servers, puts it in the cache and sends a reply to the OS who in turns sends the information to the browser. The data is then downloaded. The www part lets the browser know that you want to access the World Wide Web.

The whole process is instantaneous. The domain name system was designed to be quick and efficient. DNS could be said to be one of the most important parts of the internet, the internet would not be so predominant in our lives without it.

2.3 Internet Corporation for Assigned Names and Numbers

ICANN is the Internet Corporation for Assigned Names and Numbers, they are a non-profit organization who coordinated the DNS and created the registrar market. The majority of registrars today are ICANN accredited which means the registrar entered in to an accreditation agreement and they are governed by the policies of ICANN, therefore these registrars are contractually obliged to conform to minimum standards. The agreement is called the Registrar Accreditation Agreement and it contains the obligations imposed on the registrar by ICANN. These obligations include investigating malicious conduct, updating the WHOIS database, offering the WHOIS database search and submitting data to the domain registries. ICANN oversees registrars who are registering domain names. When a registrar is registering a domain name for a client they have to agree to terms and conditions that include ICANNs policy rules and procedures. When the name is registered, the registrant has to provide their contact details which the registrar will input into the domain name registry database. The purpose of the database is to hold information on all registrants so it is readily available if there is a dispute, people can search this WHOIS database to determine who the registered name holder of domain name is unless the WHOIS privacy feature is invoked and in that case the details of the registrar will be available instead. It is the duty of the registrar to keep this information in the database updated and accurate. If a registrar obtains knowledge of fraudulent activity they have a duty to suspend or block the

domain name. ICANN is expected to pursue registrars that appear to be acting irresponsibility to ensure they are taking their role seriously or else abolish their accreditation agreement. This self-governing function is optimal in a multijurisdictional online environment because registrars in one country do not have to follow orders of the court from another country.

2.4 Uniform Domain Name Dispute Resolution Policy

The Uniform Domain Name Dispute Resolution Policy (UDRP) was set up by ICANN to deal with disputes between the registrar and the domain name holder over the registration of a domain name. When a registrant purchases a domain name they have to agree to cooperate with the UDRP if there is a claim. To begin proceedings the claimant must inter alia provide evidence of bad faith. Evidence that the domain name holder acquired the name with the sole intention of selling it to the trademark holder, buying the name so the trademark holder cannot have it or purchasing a similarly confusing name of a trademark. If the claimant's accusations are true then the domain name will be transferred or cancelled. Usually it is possible that a registrant may move their domain name to another registrar but this is not allowed during administrative proceedings and for 15 days after. The UDRP only deals with the question of who has the best right in the domain name. It does not address potentially unlawful content on a website accessible through the domain name.[16]

2.5 Internet Intermediaries

Great numbers of people want to be connected to the internet and this is facilitated by internet intermediaries. In order to manage the large numbers of people and different services, internet intermediaries are separated into different classifications. The Organisation for Economic Co-operation and Development (OECD) categorised intermediaries into internet access and service providers, data processing and webhosting providers including domain name registrars,

[16] 'Uniform Domain Name Dispute Resolution Policy' (*ICANN*, 1999) <http://archive.icann.org/en/udrp/udrp-policy-24oct99.htm> accessed 6 August 2016.

internet search engines, e-commerce intermediaries, internet payment systems and participative networking platforms.[17] The function of internet intermediates is to provide an infrastructure to enable online exchange of information. According to the OECD, internet intermediaries are organisations which "bring together or facilitate transactions between third parties on the Internet".[18]

The OECD noted in their report that it is important to know that the nature and role of internet intermediaries is evolving and likely to change considerably.[19] The growth of online crime has meant internet intermediaries are under more pressure to take responsibility for the actions of their service users for online infringement because they are facilitating the acts. These intermediaries are in a position to impede unlawful activity on the internet by blocking and filtering content. Legal action can be initiated and the intermediaries may be forced to act. If registrars or other intermediaries do not abide they could be subject to secondary liability for facilitating unlawful activity, such as copyright infringement as seen in *The Pirate Bay*[20] case, which is discussed in chapter 4.[21] Knowledge is a crucial factor in determining this liability. It is generally believed that intermediaries should not be held liable because of the ever changing nature of the internet and the vast amount of content on it.[22] It is impossible for them to monitor activity of its users as this would drain resources.

[17] The Organisation for Economic Co-operation and Development, 'The Economic and Social Role of Internet Intermediaries' (2010) <https://www.oecd.org/internet/ieconomy/44949023.pdf> accessed 6 August 2016. p.9.
[18] *Ibid*.
[19] *Ibid*. p.4.
[20] *The Pirate Bay* case (B 13301-06) [2009] Stockholm District Court.
[21] 4.2.2.
[22] Alex Comninos, 'The Liability of Internet Intermediaries in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain' (2012) p. 6 <http://www.apc.org/en/system/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL.pdf> accessed 27 August 2016, 'Illegal Online Content And Liability Of Internet Intermediaries: Why The Messengers Should Not Be Shot' (*Diplomacy*, 2012) <http://www.diplomacy.edu/blog/illegal-online-content-and-liability-internet-intermediaries-why-messengers-should-not-be-shot> accessed 27 August 2016.

2.6 Domain Name Registrar

A registrar is an ICANN accredited entity whom one purchases a domain name from. An accredited ICANN registrar signed the Registrars Accreditation Agreement (RAA) that governs the relationship between the registrar and ICANN. In turn, ICANN has authorised this body to sell domain names on their behalf. A registrar can be seen as the middleman between the registry operator and the registrant. Registry operators have the duty of looking after each of the TLD registries, such as the .com registry and .org registry and the registrant is the entity who purchases the domain name. When you obtain this domain name, you are not buying the name outright but rather you acquire the rights to use it. The person who buys the domain name will pay a recurring fee to the registrar to keep the name registered for their use. Resellers are third party companies that a person or organisation can purchase a domain name from, resellers operate through a registrar but are not registrars themselves and have no agreement with ICANN. It is the registrars that are accountable for the resellers.

Authorities are currently trying to find the best solution to deal with online infringement. Internet service providers (ISPs) have been the target for many claims from copyright holders as they are the passage between the alleged infringer and the content. The difference between a domain name registrar and an ISP is not always clear to internet users because companies can offer both services and it is not necessary to know their separate roles. It only becomes relevant for liability, and intermediary liability is becoming a more frequent issue. An ISP provides access to the internet by supplying the telecommunication lines for certain areas of a country. ISPs buy bandwidth from national providers and offer it to internet users via network connections. This connection allows people to connect and use services and see content online as well as sharing information if they wish. ISPs block websites by redirecting requests for a domain name to a different IP address on an alternative server. While a registrars function is to offer domain names

and collect registrant information. They can block a website's domain name by removing the domain name registration from the registry.

Until recently, domain name registrars were able to elude liability for disputes because it was believed they were so far removed from the content but as we can see from recent case law, they are not safe anymore. In *KeySystems*[23], the registrar was forced to stop copyright infringement and their only option was to restrict access to the whole website by blocking the domain name. Registrars are now being put under pressure to remove domain names because they are registering names which infringe on trademark law and registering domain names for websites which are used to infringe copyright law.

[23] *Universal Music v Key-Systems GmbH* [2014] Regional Court of Saarbrücken.

Chapter 3 – Registration and the Law Regarding Registrars

3.1 Chapter Introduction

This thesis focuses on accredited registrars and chapter three looks at a registration contract from Blacknight Solutions, an ICANN accredited registrar based in Ireland.[24] It is well advised for a domain name purchaser to opt for an ICANN accredited registrar because these registrars must abide by rules and regulations laid out by ICANN which must be incorporated into the registrar's terms and conditions. The agreement contains the obligations required from the registrant in relation to their domain name and the power of the registrar to act when they deem it necessary. These terms and conditions must be agreed upon before a registrant can purchase a domain name.

As well as the registrar accreditation agreement between ICANN and the registrar that was previously discussed and the contract between the registrar and the registrant, there are laws in place to protect internet intermediaries and also intellectual property rights holders. Previously the courts applied traditional laws to determine the liability of online intermediaries but this was difficult and unjust as the situation is much different from an offline setting, for example different means and methods are used to distribute unlawful material.[25] With the advancement of technology, new laws were implemented in Europe in the form of directives to govern the online environment more effectively. We now have EU legislation which is more appropriate to determine liability online. The E-Commerce Directive[26] manages exemptions from liability and the

[24] 'Irish & European Domain Registration' (*Blacknight.com*, 2016) <https://www.blacknight.com/> accessed 23 June 2016.
[25] *Bridgesoft v Lenior* (1996) District Court of Rotterdam – Dutch case where a bulletin board operator was liable for copyright infringement without consideration for the role as an internet intermediary.
[26] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000).

Enforcement Directive[27] and the Copyright in the Information Society Directive[28] deals with civil remedies for infringements of IPRs. These directives will be discussed in this chapter along with other applicable laws.

3.2 Registration Agreement

In an attempt to limit their liability, registrars issue a contractual agreement between themselves and the registrant because without this agreement the registrar is subjecting himself to the possibility of legal accountability for the actions of the registrant. Each registrar has their own personal agreement but it must contain provisions of ICANN. The main purpose of the agreement is to protect the registrar and it contains appropriate action to be taken when websites are engaging in illegal activity.

Registration agreements are usually all quite similar; as an example this thesis looks at Blacknight Solutions service agreement. By using the registrar's service the domain name owner agrees to all terms and conditions of the agreement, including ICANNs UDRP, as well as rules, policies and agreements which ICANN, the registries or governments may enforce. This means that the registrant cannot hide behind the shield of the registrar and they are responsible for their own actions. The objective of the agreement is for the registrar to attempt to free themselves from all legal responsibility, damages and court fees resulting from the registrant infringing a third party's rights when using their service. The contract stipulates that the registrar accepts no responsibility for representations and trademark liability, even stating that registering a domain name with a registrar will not protect a registrant from liability. In case a situation would arise, the registrant may be required to provide an indemnity. Providing this assurance means the registrar will not be subject to the costs personally which could impact business. The registrar reserves the

[27] Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004).
[28] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001).

right to reject or terminate the service for any reason within, in Blacknight's case, 30 days post commencement of contract. They are allowing themselves to act in ways they believe necessary to avoid accountability but their actions must be carefully decided as aspects of this contract may not be valid against fundamental rights, such as the freedom of expression which is superior to the agreement. The registrar's agreement goes beyond legitimate limitation regarding freedom of expression. After these 30 days have lapsed, the registrar states they may suspend or cancel the service for any reason without restriction and they provide a non-exhaustive list including registering a prohibited domain name, non-payment, abuse of the service, allegations of illegal conduct and violation of their ISPs user policy. This gives registrars the discretion to act ethically if it is clear the registrant is engaging in unlawful activity. Registrars can terminate the contract after 30 days' notice, allowing the registrant to transfer their domain name to another registrar. This is one of the reasons why targeting domain name registrars is considerably ineffective. If the registrar acts upon notification of illegal activity, the registrant has the opportunity to move to another registrar and their content is still online. The registrant must agree that when the domain name is registered it can be subject to suspension, cancellation or transfer by any ICANN procedure, any registrar or any registry administrator procedures approved by ICANN. The registration does not create a property interest, when a registrant purchases a domain name they are merely obtaining the rights to use the name.

By agreeing to these terms and conditions, the user is agreeing to not subject the registrar to any claims or harm. The registrar will not check if the domain name infringes a trademark or if the name is prohibited as it is the registrant's responsibility to establish the legality of the domain name.[29] If the situation would arise that the registered domain name does infringe on someone's legal rights, then the registrar may be required by request of the court or UDRP to terminate or transfer the domain name. The user is agreeing to the UDRP and an account can be suspended,

[29] *Association Francaise pour le Nommage Internet en Coopération*, Paris Court of Appeal, 19 October 2012.

transferred or cancelled based on the outcome of the dispute resolution. The information provided by the registrant must be complete and accurate, this allows for an accountable system with transparency. Accurate information makes a reliable WHOIS search so it is quick and easy to contact the domain name owner if there is an infringement. The registrar reserves the right to place a registrar lock on the domain name if they decide it is crucial. A registrar's lock prevents a domain name from being transferred.

LegitScript and Knujon published a report where they investigated how domain name registrars react when a request is sent to them to suspend domain names of unlawful websites that they had registered.[30] In the report the registrars were asked to enforce their own terms and conditions. The paper was aimed at rogue internet pharmacies who were selling counterfeit drugs, drugs without prescriptions and websites claiming to have a pharmacy licenses. The authors of the report contacted registrars with evidence of fraudulent activity and reported on their response. Eleven registrar promptly acted. For example, GoDaddy, a US based registrar conducted an independent review and based on the results acted in accordance with its own terms and conditions. Five registrars kept the websites online even though the activities were against their policy. Being an ICANN accredited registrar means that the registrar is forbidden from allowing registrants to use their domain names to direct internet users to illegal content and this is incorporated into the registrar's terms and conditions. If a registrar becomes aware of unlawful activity they have a duty to suspend the domain name.

Registrars have a self-policing obligation which is supposed to balance the freedom of expression with innovation. The contract between the registrar and the registrant gives the registrar the opportunity to take a proactive rather than reactive role in stopping illegal conduct while also protecting themselves. The terms and conditions give the registrar contractual rights to

[30] LegitScript and Knujon, 'Rogues and Registrars: Are Some Domain Name Registrars Safe Havens for Internet Drug Rings?' (2010) <http://www.legitscript.com/download/Rogues-and-Registrars-Report.pdf> accessed 23 June 2016.

suspend, lock and transfer the domain name, but it appears that registrars are declining to enforce their own restrictions. They have the opportunity to enforce their terms and conditions but are not, this may be due to the lack of incentive to do so. The terms and conditions characterise the legal relationship between the registrar and the registrant. As well as the private contract, there is legislation in place in the EU to deal with internet intermediaries who are acting in their capacity. The Commission drafted the directives and it was up to the Member States to implement these into their national legislation taking their own country's social and cultural norms into consideration.

3.3 Relevant Law

3.3.1 E-Commerce Directive

The internet is a dynamic and progressive tool for communication. To protect the capabilities of the internet we require legal policies, these policies are put in place to allow the internet to thrive. The E-Commerce Directive was created to develop greater legal certainty for information society services and to establish harmonised rules within the European Union for this field. An information society service is "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[31] Directive 2000/31 enhances the role of self-regulation and acts as a safe harbour for internet intermediaries by outlining limitations of liability in Articles 12 to 15.

The E-Commerce Directive's limitations on liability for internet intermediaries acts as a safeguard for them while acting in their role. This helps them not to take disproportionate actions out of fear of liability for their client's actions as this would impede fundamental rights of the people. It has been welcomed by intermediaries as it allows them to conduct business without the fear of undue liability. The directive was kept abstract to accommodate for the fast changing nature of the electronic world but this is its downfall because it is difficult to construe as the directive does

[31] Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provisions of information in the field of technical standards and regulations.

not give a legal definition of an online intermediary. It is tough to interpret the directive in light of domain name registrars because they do not clearly match the wordings of the applicable articles.

Article 12 relates to 'mere conduit' providers. It gives the service provider a safe harbour where they will not be liable for information transmitted, on the condition that the provider does not initiate the transmission, does not select the receiver of the transmission and does not select or modify the information contained in the transmission. The transmission includes the automatic, intermediate and transient storage of the information transmitted if its purpose is for carrying out a transmission in the communication network and once it is not stored for longer than necessary. Article 12(3) of the directive notes that the article should not affect a court or another legal entity within a Member States legal system to require the service provider to terminate or prevent an infringement. *EMI v UPC*[32] is an Irish case where the court considered this Article 12 as a defence for ISPs. EMI requested that UPC, which is an ISP, to implement a three strike system where the ISP would send notifications to internet users who were found to engage in unlawful peer-to-peer file sharing. UPC did not comply as it deemed they were a 'mere conduit' provider and had no control over the communications. EMI then sought an injunction to cut of internet access to certain users and to block access to particular websites. Justice Charlton held that the demands by EMI were not permissible under Irish law.

Article 13 makes reference to 'caching' providers, this article allows for service providers to temporarily store information provided for the sole purpose of making more efficient information transmission to other recipients of their service. With the conditions that the provider does not modify the information, the intermediary complies with conditions on access to the information, the information is updated regularly, there is no interference with the lawful use of technology used to obtain the information and the service provider acts quickly to remove or disable access

[32] *EMI Records (Ireland) Limited et al v UPC Communications Ireland Limited*. Irish High Court Case. No. 2009/5472P.

to the content if they obtain knowledge of illegal content or if they are requested by the court to remove or disable.

Article 14 of Directive 2000/31 deals with 'hosting' providers who store data from their users. Member States shall ensure that the information society service provider is not liable for the stored information provided:

"(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information".[33]

Host providers may store information from the recipients of their service and not be liable for the content provided they have no knowledge of illegal activity or information stored. If the hosting provider gains this knowledge then they have a duty to act quickly to remove or disable access to this information. Article 14 acts as a safe harbour for hosting providers. Hosting can cover an array of services and a service provider will fall under Article 14 if they store information that the recipient of the service created. The OECD classified domain name registrars in the same category as hosting providers. Registrars fit into this category as they store details of the domain name registration in the registry's database and that maps domain names to IP addresses. The host providers must also act expeditiously when knowledge is obtained, the Directive has no timeframe but article 46 states:

> "In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information

[33] Article 14(1) of Directive 2000/31/EC.

concerned; the removal or disabling of access has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information".

It is logical to expect them only to respond to court orders because registrars do not have the knowledge to examine trademark and copyright infringement, their role is to provide domain names passively.

The issue of actual knowledge was examined in *L'Oréal v eBay*.[34] This was a UK case where L'Oréal claimed that eBay permitted users to sell counterfeit goods and therefore eBay was infringing upon their trademark rights, "the service provider must have actual knowledge of, and not a mere suspicion or assumption regarding, the illegal activity or information."[35] Actual knowledge is difficult to interpret, it is attained through an investigation by the intermediary, through a notification or through an active role. The notification element requires precision and substantiation but guidelines need to be established. Clarity of the actual knowledge needs to be given to avoid the article being misused by competitors. The Electronic Frontier Foundation stated that a Digital Millennium Copyright Act (DMCA) report in 2006 found that almost 60% of takedown notices received by Google were from company competitors.[36] This may be avoided if the person issuing the notification first gets a judicial inquiry to determine the unlawful content.

Article 15 provides that service providers have no general obligation to monitor.

---

[34] *L'Oréal SA and Others v eBay International AG and Others* [2011] CJEU C-324/09.
[35] *Ibid.* par. 162.
[36] Gwen Hinze, 'Submission of The Electronic Frontier Foundation on the Consultation on the EU E-Commerce Directive (2000/31/EC)' (2010) P. 5 <https://www.eff.org/files/filenode/international/effeuecommercedirectiveconsultationresponse.pdf> accessed 1 August 2016.

"1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements."

Art. 15(1) states that Member States shall not impose a general obligation on service providers who are protected by articles 12 to 14 to have a duty to monitor information or to actively seek out illegal activity The first paragraph is valuable to registrars who would otherwise have to check the legality of the domain name when registered, for example if 'perscriptionfreepharmacy' was a new registration then the registrar would have to conduct an inquiry. The second part of 15(1) where there is no obligation to actively seek out illegal activity applies to registrar's because they do not have to look for information in the DNS data. 15(2) of the article states that Member States may oblige the service providers to inform the competent public authority in relation to illegal activity by recipients of their service. This article was designed to not put an overly burdensome duty on internet intermediaries and also to protect citizen's right to privacy which is a fundamental right. In the *Netlog* case[37], an injunction was banned by the CJEU because it would require the hosting service provider to generally monitor the data of its users and this breached article 15(1) of the E-Commerce Directive. Netlog was a social network so it was considered a hosting platform that stored information of its users.

[37] *SABAM v Netlog* [2012] CJEU C-360/10

The purpose of the directive is to allow service providers on the internet to maintain a technical, passive role which will allow them to keep developing the infrastructure of the internet, this is due to the fact that while providing their service to customers they can technically infringe on copyright law without having knowledge of it. The directive protects internet intermediaries providing an inactive role so if they began to monitor the content of their service they no longer have protection under the E-Commerce Directive.

As Schellekens notes[38], this demand for a duty of care creates a slippery slope for internet intermediaries because they then would have an active duty of care meaning they have greater influence and control over the internet. This could lead to a disproportionate restriction on future economic activities on the internet and it could contribute to more legal uncertainty. It would be unfair to argue that the registrars should monitor all the registrant's activity or be liable considering all the domain names that have been registered. Registrars are not trained to monitor criminal activity and with the risk of liability, they will always take the safe option for themselves and remove a domain name. This is a problem for freedom of expression. Sjoera Nas, the Director of the Dutch liberty organisation Bits of Freedom directed a research study of the EU safe harbour and noted "the European legislation leaves plenty of room for doubt and misguided judgement by providers". [39] The directive was designed to create greater legal certainty and to create harmonization within the EU but the position within Europe is still unclear and it is still a relatively new area. The directive is vague but has been successful so far as it allows for flexibility in order to effectively respond to technological developments and change in internet intermediaries.

[38] Maurice Schellekens, 'Liability of Internet Intermediaries: A Slippery Slope?' (2011) 8 SCRIPTed <http://www2.law.ed.ac.uk/ahrc/script-ed/vol8-2/schellekens.pdf> accessed 23 June 2016.
[39] William Lehr and Lorenzo M Pupillo, *Internet Policy and Economics* (Springer 2009), p.90.

3.3.2 Enforcement Directive

The purpose of the Enforcement Directive is to combat intellectual property right infringements. Article 11 stipulates that Members States shall ensure that judicial authorities may issue an injunction against the infringer to prohibit the continuation of the infringement and may be subject to a penalty. Rights holders may also apply for an injunction against the intermediaries who facilitate the infringement of an intellectual property right. The Directive does not disturb the E-Commerce Directive, particularly Articles 12 to 15.[40] Article 3 of Directive 2004/48 has limitations to enforcement of IRPs, for example a wide-range monitoring obligation would clash with Article 3 of the Enforcement Directive because it would not be "fair and equitable".[41] In *Scarlet Extended*, the CJEU held that an injunction requiring an ISP to install a global filtering system to monitor all electronic communications going through the network without a limitation on time would be an infringement of the ISP to conduct business and this would be incompatible with Article 3(1) of the Enforcement Directive.[42] It states that the measures, procedures and remedies shall be fair and reasonable without unnecessary delays. They must also be proportionate and be applied in such a way as to avoid the creation of barriers to legitimate trade.

3.3.3 Copyright in the Information Society Directive

Article 8(3) of the Copyright in the Information Society Directive (also known as the InfoSoc Directive) reiterates Article 11 of the Enforcement Directive for Copyrights, stating that Member States shall ensure rights holders are in a position to apply for an injunction against intermediaries whose services are used to infringe copyright or related right. It is explained in recital 59 that intermediaries are in the best place to bring infringements to an end therefore rights holders can apply for an injunction against intermediaries who carry out third party infringement. In *Telekabel*

[40] Article 2(3) of Directive 2004/48/EC.
[41] Article 3(1) of Directive 2004/48/EC.
[42] *Scarlet Extended SA v Belgian Society of Authors, Composers, and Publishers (SABAM) [2011] CJEU C-70/10.* par. 48.

Wien[43], the defendants, in their appeal, commented that their services could not be considered to infringe copyright with the meaning of Article 8(3) of the directive because it did not have any business relationship with the operators of the website.[44] The InfoSoc Directive tries to not only end infringements but also to prevent them in the future which is acknowledged in *L'Oréal v eBay*, the judge states that in view of Directive 2004/48, national courts must allow service providers to be not only ordered to bring an end to infringement but to also prevent further infringement.[45] Both the Enforcement Directive and the InfoSoc Directive allow rights holders to seek an injunction if there is an infringement of their copyright but the legal basis of the injunction they may apply for is not detailed as this is left up to national law and the Directive provides merely a remedy.

3.3.4 Other Relevant law

Besides the mentioned directives, there are certain EU laws that a registrar needs to respect when acting in their role as an internet intermediary. Suspending a domain name for a breach of intellectual property rights can conflict with the right to freedom of expression under article 17(2) of the EU Charter of Human Rights, as well as this it can conflict the freedom of information found in article 11 of the Charter and article 10 of the European Convention of Human Rights. The right to conduct business is enshrined in article 16 of the EU Charter so this also needs to be recognised. There may also be situations where it can disturb the right to privacy under article 8 of the Charter if registrars have to pass on contact information about a registrant, but this is rare because the details are usually publicly available unless the WHOIS privacy feature is invoked. Data privacy is important to consider when issuing an injunction. The Article 29 Working Party noted an injunction to employ a filtering system that would store all traffic data related to copyright could be a breach of data privacy. A fair balance needs to be struck between

[43] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12.
[44] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12. par.16.
[45] *L'Oréal SA and Others v eBay International AG and Others [2011] CJEU C-324/09.* par. 131.

fairness, proportionality and equitability. As well as being obliged by EU law, registrars are even under contract to prohibit unlawful website activity in order to remain an accredited registrar.

3.4 Chapter Conclusion

It appears within EU law that the legislators are unclear about registrars' position. It also seems that registrars are uncertain about their role. In Rogues and Registrars[46], a registrar, UK2Group, was issued with a complaint and responded by saying that the authors should contact an approved Domain Name Dispute Resolution Provider to submit a complaint. This company did not understand ICANNs rules, UDRP and the law. The UDRP is there to deal with trademark claims but there is not redress for unlawful activity on the website. Registrars should be well informed that the UDRP deals with trademark infringement and all other complaints have to be dealt with through an alternative procedure. If a registrar does not have the competence to understand the UDRP then they should not be legally obliged to judge IPR infringements without the involvement of a judicial authority. Domain name registrars are the backbone to the internet as we know it and registrars are unsure where they stand in terms of content liability. The E-Commerce Directive heightens competition around Europe for service providers because it allows them to act in their daily role without the worry of being liable. They should have an active role in removing domain names if they are aware they are facilitating fraudulent activity. If they take no action they are holding themselves to the possibility of secondary liability. A situation where the registrar should legally be held accountable for the actions of the registrant is when they invoke the anonymous WHOIS privacy feature.[47] This is a facility that allows the registrar to input their own contact information rather than the true registrants details for the purpose of privacy. It was originally introduced to prevent spam and phishing but it now is used more for deterring litigation

[46] LegitScript and KnuJon, 'Rogues and Registrars: Are Some Domain Name Registrars Safe Havens for Internet Drug Rings?' (2010) <http://www.legitscript.com/download/Rogues-and-Registrars-Report.pdf> accessed 23 June 2016.
[47] Privacy And Proxy Services' (*Whois.icann.org*, 2016) <https://whois.icann.org/en/privacy-and-proxy-services> accessed 23 June 2016.

and avoiding accountability for unlawful material. This function undermines the purpose of the WHOIS database. In LegitScript's report[48], the authors had to contact the registrar directly to tell them that one of their registered domain names was selling prescription drugs without a valid prescription because registrant's details were hidden. It was clear that in this instance, the proxy domain registration was being used to circumvent the law. In EMI v UPC, the Judge held that to block peer-to-peer filing sharing websites outright would not be proportionate in preventing copyright infringement and could suppress the right to communication on the internet.[49] Registrars should be immune from liability when they are not involved. It should be necessary for them to block a domain name by an order of the court after it has been established that the material is illegal as this gives greater legal certainty as the E-Commerce Directive does not provide guidance when determining what is unlawful.

[48] LegitScript and KnuJon, 'Rogues and Registrars: Are Some Domain Name Registrars Safe Havens for Internet Drug Rings?' (2010) <http://www.legitscript.com/download/Rogues-and-Registrars-Report.pdf> accessed 23 June 2016.
[49] *EMI Records (Ireland) Limited et al v UPC Communications Ireland Limited*. High Court Case. No. 2009/5472P.

Chapter 4 – Weighing up Rights

4.1 Chapter Introduction

The aim of domain name blocking is to stop internet users from having access to content on a website. If the domain name is blocked, when a user enters the name into the browser it will not direct them to the website. Registrars can take down or suspend domain names relatively easily and quickly but it should be thought through carefully before proceeding as blocking a domain name will have an impact on all the content on a website and the services it provides. Having a block will put a stop to emails for the domain to be sent or received and all the webpages of the domain will be blocked including subdomains so it may include both legal and illegal content. Domain names are important to the functionality of the internet. Their ease of use for accessing not only websites but also emails and other services makes them an essential element to the evolution of the internet. As well as this, suspensions and take downs can result in over blocking, which causes limited access to lawful content.

There has been demand for registrars to help deal with the issue of unlawful content online by using their power to restrict access to websites. It is believed they are in a good place to take control because of their contractual relationship with infringers who have registered domain names with them. Registrars can invoke the terms and conditions of their registration agreement which registrants must consent to before registering the domain name. Registrars are opposed to the idea of taking the responsibility for their client's activities but they are in a good position to act, especially on foreign websites where it would be almost impossible to issue a court order for an injunction. As well as this, domain name registrants rely on internet users using the domain name to get to the content and blocking access to the name would inhibit many internet users from navigating their way to the website. Blocking a domain name needs to be carefully decided because doing so erroneously could have serious implications.

There are rights that need to be considered first and the action taken must be proportionate and fair. This chapter firstly looks at fundamental rights. Registrars have the freedom to conduct business including the right to innovation and the public have a right to freedom of information and expression. These rights are superior to all other legislation within the European Union. The second part of this chapter considers the important elements of balancing, effectiveness and proportionality when it comes to domain name blocking.

4.2 Fundamental Rights

4.2.1 Freedom to Conduct Business

The freedom to conduct business is protected by Article 16 of the EU Charter, it states "the freedom to conduct business in accordance with Union law and national laws and practices is recognised"[50], meaning that a required function of a domain name registrar should not unduly impede on their entrepreneurship and innovation. It was discussed in *UPC Telekabel Wien*[51], "an injunction such as that at issue in the main proceedings contains its addressee in a manner which restricts the free use of the resources at his disposal because it obliges him to take measures which may represent a significant cost for him, have considerable impact on the organisation of his activities or require difficult and complex technical solutions".[52] In this case, the Court considered the cost as an aspect of the freedom to conduct business because cost is a part of an organisation's resources. *UPC Telekabel Wien* concerned an Austrian internet service provider, UPC Telekabel GmbH and Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH. Constantin Film and Wega, the claimants, requested that Telekabel block access to a website that internet users were using to watch copyrighted films which Constantin Film were the rights holders to. Telekabel failed to act even though they acknowledged that there was

[50] Charter of Fundamental Rights of the European Union 2009.
[51] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12.
[52] *Ibid,* par. 50.

copyrighted material on the website and the claimants began proceedings before the Vienna Commercial Court seeking a court order to stop UPC Telekabel allowing their users to access the website. The court gave an order to block the domain name system access to the domain and to all current and future IP addresses related to that website that Telekabel knew of or would gain knowledge about. This was appealed to the Vienna Higher Regional Court and the Court revised the order and forbid access to the website without specifying the concrete means of implementation. The Court required Telekabel to provide a result but left it up to them to decide how they would implement the order. An injunction on UPC Telekabel could impede the freedom to conduct business because of the pressure on resources and the expense and complex technology required. Telekabel appealed to the Supreme Court which stayed its judgement and referred questions to the CJEU for a preliminary ruling because of the lack of legal certainty. The CJEU felt that the injunction was fair and balanced, they believed it did not impact the freedom of an ISP and Telekabel were in the best position to choose most suitable means of implementation. There was no guidance given except what is in the legislation.

Article 3(2) of the Enforcement Directive states that "measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse".[53] This was applied in *L'Oreal v eBay*[54] where the CJEU expressed that having an injunction on a marketplace would be seen as a barrier to legitimate trade and that is not allowed by the Enforcement Directive. In the case of *Scarlet Extended SA v SABAM*[55], the ISP was requested to implement an expensive filtering system and it was rejected by the CJEU because of the enormous cost. The case involved Scarlet Extended SA which is an ISP and SABAM which is a Belgian management company in charge of permit use of musical works of authors,

[53] Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004).
[54] *L'Oréal SA and Others v eBay International AG and* Others [2011] CJEU C-324/09.
[55] *Scarlet Extended SA v Belgian Society of Authors, Composers, and Publishers SCRL (SABAM)* [2011] CJEU C-70/10.

composers and editors to third parties. SABAM noticed that Scarlets customers were downloading work of SABAM illegally through a peer-to-peer file sharing network. SABAM requested that the Brussels Court of First Instance required that Scarlet Extended, the ISP, to end the copyright infringement. The Court issued an injunction and as well as this a periodic penalty. Scarlet appealed to the Brussels Court of Appeal stating that the injunction did not comply with EU law as it imposed a general obligation to monitor communications on its network and this was inconsistent with Article 15 of the E-Commerce Directive[56] and it breached the protection of personal data[57] which is a fundamental right. The Court of Appeal asked the CJEU if EU law permits Member States to order ISPs to install a system to filter all electronic communications to identify illegal files as a method to prevent copyright infringement for an unlimited time at the expense of the ISP. The CJEU stated that firstly, IPR holders may apply for an injunction against intermediaries under article 8(3) of the InfoSoc Directive[58] and Article 11 of the Enforcement Directive[59] if their rights are being infringed by a third party. Secondly, the Court pointed out that the national courts can order intermediaries to take action to bring an end to infringement. However, the limitations of the InfoSoc Directive[60], the Enforcement Directive[61] and the rules recognised by the Member States shall not interfere with the provisions of the E-Commerce Directive. The CJEU held that the injunction would seriously interfere with Scarlet freedom to conduct business because of the intricate and costly filtering system. "...such an injunction would result in a serious infringement of the freedom of the ISP concerned to conduct its business since

[56] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000).
[57] Charter of Fundamental Rights of the European Union 2009, Article 8.
[58] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001).
[59] Directive 2004/48/EC.
[60] Recital 16 of Directive 2001/29/EC.
[61] Article 2(3) (a) of Directive 2004/48/EC.

it would require that the ISP install a complicated, costly, permanent computer system at its own expense... ".[62]

In *Promusicae v Telefónica de España*[63], when the Court was considering the freedom to conduct business, they held that it was not appropriate to balance it against IPRs because of the cost of enforcing a system to stop copyright infringement would be too costly and complicated.

Having registrars liable for the actions of their users suppresses innovation because companies, especially smaller ones, will struggle to pay for a legal team and will not have the resources to devote time into investigating all possible infringements. It can also deter registrar because of the possibility of a heavy obligation, with it comes more costs and stricter licensing. Registrars could erroneously block a domain name for an organisation who was lawfully online which suppresses the organisations innovation. If registrars did not fear liability they would not be under pressure to block domain names, this is good for innovation because it allows the growth of the information society. The EFF in their submission of the consultation of the EU E-Commerce Directive stated that the limitations on liability of Internet intermediaries was fundamental for innovation.[64] Directive 2000/31 furthers innovation through the development of e-commerce within the EU by harmonising legislation and encouraging free movement of services.

For registrars, blocking domain names to prevent illegal content is easy to do and that is why they are becoming more popular. Nonetheless, it does restrict a registrar's freedom to conduct business when they are required to examine cases of infringement. It uses up resources and restrains their freedom to innovate. This is because a decision by a registrar to block a domain name should involve careful consideration so as to protect the public's freedom of expression.

---

[62] *Scarlet Extended SA v Belgian Society of Authors, Composers, and Publishers SCRL (SABAM)* [2011] CJEU C-70/10, par. 48.

[63] *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] CJEU C-275/06.

[64] Gwen Hinze, 'Submission of the Electronic Frontier Foundation on the Consultation on the EU E-Commerce Directive (2000/31/EC)' (2010) <https://www.eff.org/files/filenode/international/effeuecommercedirectiveconsultationresponse.pdf> accessed 1 August 2016.

Registrars have a duty to act upon obtaining 'actual knowledge' of an infringement.[65] Any third party's submission of notice of copyright infringement cannot amount to actual knowledge as the registrar still has to carry out an investigation. It would be more pragmatic to oblige registrars to respond to court ordered removal as this would eliminate an attempted legal analysis that may result in over-blocking out of fear of the potential cost of liability. The registration market is a competitive place and registrars do not have the resources to investigate all claims. Registrars may block domain names without an investigation to save time and money. This can become an easy route for people to censor content online.

There is no clear position yet of the CJEU when trying to balance the freedom to conduct business with Intellectual Property Rights but we can see from *Telekabel*[66] that when the service provider has been aware of the infringement then it is more likely that an obligation will be imposed. The registrar should have a duty to investigate upon receiving a substantiated notification. It should be from a legal authority because this would provide an unbiased account of the alleged infringement with legal certainty. It would have to provide detailed evidence of the claim. The notification would have to be weighed up against freedom of expression because access to all content will be revoked with a domain name block. It would be impossible to investigate all claims without impinging on the registrar's freedom to conduct business. If they were obliged to review all claims then they could not invest an adequate amount of resources into each one, leading them to block a domain name upon notification from any third party. The registrar cannot assume allegations to be correct as they should have a minimum duty to investigate to ensure they are not removing lawful content and restricting the freedom of expression. In 2004, Bits of Freedom conducted an experiment to evaluate how ISPs reacted to notice and takedown notifications. The researchers sent fake notifications to 10 ISPs about a work

[65] Article 14 (1) (a) of Directive 2000/31/EC.
[66] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12.

that already belonged to the public domain. The result was that 7 out of 10 providers took down the content without an inquiry.[67] Having a judicial review ensures a critical assessment.

4.2.2 Freedom of Expression

> Article 11(1) of the EU Charter reads:
>
> "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".[68]

This Article stipulates that every person has the right to impart and receive information without intrusion. Freedom of expression is also included in the European Convention of Human Rights under Article 10 and the Article contains restrictions and conditions that are prescribed by the law and necessary in a democratic society.[69]

In the Advocate General's opinion on *Telekabel*[70], he wrote that included in the right to freedom of expression was the right to access to the internet, he declared it an essential right. "...the right to Internet access is protected in theory by the constitutional guarantees applicable to freedom of expression and freedom to receive ideas and information. In the view of the ECHR, the Internet plays an important role in enhancing access to news and facilitating the dissemination of information".[71] Suspending a domain name as whole could breach a person's right to freedom of expression and information because they may be blocking access to lawful information online. Blocking access to legitimate content would be a breach of this fundamental right. As discussed in *Telekabel*[72], enforcement measures of the registrar must be targeted. The Advocate General

[67] S. Nas, 'The Multatuli Project: ISP Notice and Take down' (2004).
[68] EU Charter of Fundamental Rights 2009.
[69] *Ibid,* Article 10(2).
[70] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12.
[71] Opinion of Advocate General of *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH,* par. 108.
[72] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12.

opined that there was concern that the service provider might choose an intrusive means and this would cut into the freedom of information of the users because of the fear of what would happen if the order was not obeyed.

In the UK case of *Twentieth Century Fox Film & Others v BT*[73], BT alleged that an injunction to block the whole website was disproportionate. Justice Arnold disagreed and said that if the infringement is on a massive scale then it is suitable to block the whole website. This case involved a file sharing website called Newzbin2 where most of the content was works that Twentieth Century Fox owned copyright to. Justice Arnold stated that the protection of IPRs was more important than the freedom of expression.[74] It was held that the injunction to be imposed was proportionate because under Article 1 of the first protocol of the ECHR[75], the right to the peaceful enjoyment of his possessions, including copyright, outweighed the rights of Newzbin2's users and operators. This situation differed from the others mentioned because there had already been an injunction granted for the original website Newsbin.[76] *Newzbin2* case was a test case for an injunction granted against an ISP.

Yildirim v Turkey[77] is a case that was before the European Court of Human Rights. It concerned the first ever case of a violation of freedom of expression on a web 2.0 platform. In this case, a Turkish court had arranged as interim injunction to block access to a website that had hateful content regarding the founder of the Turkish Republic and this was a criminal offence. The court was told that the only way to block access to the website was to block access to all of Google Sites so when this block was invoked all websites hosted by Google were blocked. The European Court of Human Rights held that restrictions on internet access outside the strict legal framework regulating the scope of the restrictions and affording the guarantee of judicial review to prevent

[73] *Twentieth Century Fox Film & Others v British Telecommunications PLC* [2012] 1 All ER 806.
[74] *Ibid.* par. 169
[75] European Convention on Human Rights 1953.
[76] *Twentieth Century Fox Film Corporation and others v Newzbin Ltd* [2010] EWHC 608 (Ch).
[77] *Yildirim v Turkey* [2012] European Court of Human Rights (no. 3111/10).

possible abuses resulted in a breach of freedom of expression which is protected by Article 10 of the ECHR. The importance of the freedom of expression and information has been confirmed through case law. The Advocate General in his opinion in *Telekabel* expresses that the freedom to impart and receive information is necessary in a democratic society.[78]

Registrars are not trained to act as watchdogs for fraudulent activity. There is always going to be the risk that they will take the cautious option and block a domain name because of the fear of liability and this hugely impacts the freedom of expression. After *The Pirate Bay*[79] decision, numerous Swedish file sharing sites shut down voluntarily. The case of The Pirate Bay was a 2009 judgement in Sweden where fifteen claimants accused four people of promoting copyright infringement using a torrent tracking website called The Pirate Bay. An appeal was refused by the Supreme Court in 2012 and the domain name had to be changed from thepiratebay.org to thepiratebay.se. The Court stated that since the accused knew the site had torrent files on it and has responsibility for the site that the E-Commerce Directive was not applicable to them. The owners of the website were charged with being an accessory to copyright infringement. Swedish ISPs were also requested to block access to the website. The managing director of the ISP Bahnhof said "we will not censor sites for our customers; that is not our job. I am against anything that contradict the principles of a free and open internet".[80] In May 2016, the Swedish Court of Appeal ruled to have the domain names thepiratebay.se and piratebay.se revoked by the government because of the infringing copyright. The Pirate Bay have since moved back to thepiratebay.org, their original domain name. Currently The Pirate Bay still have their .se domain name but do not host on that domain, when an internet user navigates to the domain name they are redirected to the .org domain name.

[78] Opinion of Advocate General of *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH,* par. 21.
[79] *The Pirate Bay* case (B 13301-06) [2009] Stockholm District Court.
[80] 'ISPs Refuse to Shut down Pirate Bay' (*Thelocal.se*, 2009) <http://www.thelocal.se/20090418/18940> accessed 22 June 2016.

The internet is primary tool for information and expression and in *Telekabel*[81] it was ruled as a necessary medium in a democratic society. The difficultly with blocking a domain name is that all content on the website is inaccessible, lawful and unlawful. Blocking access to lawful content is the essence of the problem which will be analysed in this chapter. Blocking access to information seriously impinges on the freedom of expression. A more appropriate measure would strictly target the infringing material which does not happen with blocking a domain name.

4.3 Principles of EU Law

Registrars have the legal authority and technical ability to block a domain name, but before the registrar decides to act or the court decides to impose any measures on a registrar, there are criteria which need to be considered. A number of issues which need to be first taken into account have already been mentioned above, the freedom to conduct business and freedom of expression. Preceding an injunction or suspension it has to be established that the blocking is feasible and proportionate. According to Article 2(3) of the Enforcement Directive[82], injunctions have to be effective, proportionate and dissuasive. Article 3 of the same directive states that injunctions have to be fair and equitable.[83] Blocking or suspending a domain name cannot be done unless there is a legal basis. If the reason is to stop a user accessing the copyrighted work then it may be more efficient to consider targeting the website owner and remove the infringing content rather than taking down the whole website because access to the website should not be illegal. The scale of the infringement is an important factor to consider and that has an influence on the intrusiveness of the blocking measure.

[81] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12.
[82] Directive 2004/48/EC.
[83] *Ibid.*

4.3.1 Balancing

Article 6(1) of the TFEU[84] states that fundamental rights are guaranteed by the EU Charter and are primary union law. Article 6(3) notes fundamental rights are guaranteed by the ECHR and constitute general principles of the union's legal order resulting from the constitutional traditions common to Member States.[85] The Charter and the Convention take precedence over all other EU legislation.

When deciding whether a registrar should block a domain name, a fair balance of rights has to be established between the internet user, the copyright holder and the registrar. No rights are absolute, rather there has to be harmonisation between the conflicting rights at stake which requires due consideration. A balance of rights was deliberated in *UPC Telekabel*[86] and as well in the *Promusicae*[87] case.

> "The Court has already ruled that, where several fundamental rights are at issue, the Member States must, when transposing a directive, ensure that they rely on interpretation of the directive which allows a fair balance to be struck between the applicable fundamental rights protected by the European Union legal order. Then, when implementing the measures transposing that directive, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with that directive but also ensure that they do not rely on an interpretation of it which would be in conflict with those fundamental rights or with the other general principles of EU law, such as the principle of proportionality".[88]

[84] Treaty on the Functioning of the European Union 2012.
[85] *Ibid.*
[86] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12.
[87] *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] CJEU C-275/06
[88] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12*,* par. 46.

It was noted in *Telekabel*[89] that when issuing an injunction under Article 8(3) of the InfoSoc Directive, there has to be a balance between, firstly, copyrights protected by Article 17(2) of the Charter, secondly, the freedom to conduct business under Article 16 of the Charter and thirdly, the freedom of information of internet users who are protected by Article 11 of the Charter. Savola discussed a balancing rule in the article "Proportionality of Website Blocking"[90], the rule states that the larger the negative economic effect that the infringement causes to the rights holder, the more severe the enforcement measure that is available should be. As well as this, the loss to the rights holder should be proportionate to the cost to the provider and the impact on the freedom of expression to the service user. Savola explains the most important factors when balancing are effectiveness and cost. If the blocking is not effective it will not solve the monetary loss for the rights holder. If the blocking is not expensive or intrusive then it will not impact the service provider. The more costly and invasive it is, there is a high requirement for the justification of the effectiveness.

4.3.2 Effectiveness

When considering effectiveness in relation to domain name blocking by the registrar, the most important factor is how difficult the measure will be to bypass. Article 3(2) of the Enforcement Directive makes reference to the fact that measures enforced must be inter alia effective. As noted in *Telekabel*[91]:

"the measures which are taken by the addressee of an injunction… must be sufficiently effective to ensure genuine protection of the fundamental right at issue, that is to say that they must have the effect of preventing unauthorised access to the protected subject-matter or, at

[89] *Ibid.*
[90] Pekka Savola, *Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers* (2014) JIPITEC 116.
[91] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12.

least, of making it difficult to achieve and of seriously discourage internet users who are using the services of the addressee of that injunction from accessing the subject-matter made available to them in breach of that fundamental right".[92]

When considering how effective blocking is, it is important to bear in mind that even though it is possible to access a website after the domain name block, it does not mean that every user will do so, as discussed in *Telekabel*[93] where the Judge opined that the users may not bother to circumvent the block or will not wish to do so. A registrar blocking a domain name can decrease the number of visitors to a website but it is difficult to determine whether it is effective in stopping infringement. The majority of users of file sharing websites are technically inclined and it is likely that they will have no problem with circumventing a blocked domain name and will be able to access the website. File sharing websites such as The Pirate Bay use torrents to share files with other service users. The users can search for files on the websites then a tracker searches other users' computers for the files so there is no need for a central server. It was reviewed in *Ziggo BV and XS4ALL BV v BREIN*[94] that a blockade cannot be regarded as effective if the infringing subscriber can bypass the block by accessing the unlawful content on an alternative BitTorrent website because this shows that the number of infringements online is not decreasing but rather just the path where the users gets the content changes. It was stated that in this case the XS4ALL users access The Pirate Bay through another route.

It is important to note that blocking a domain name does not end the activity. The registrant can move to another domain name and registrar. It can lead to a constant pursuit, for example, when The Pirate Bay was told that their .se domain name was going to be blocked, they quickly switched to other domain names including thepiratebay.mn and thepiratebay.vg. Blocking a domain name does not result in a complete end to the infringement because the content can still

[92] *Ibid,* par. 62.
[93] *Ibid.*
[94] *Ziggo BV and XS4ALL BV v BREIN,* ECLI: NL: HR: 2015: 3307 par. 5.19.

be accessed through the IP address. Copyright infringement is still on the rise according to Allen-Robertson in his book on the digital culture industry.[95] Something needs to be done but targeting domain names may not be the most effective approach. Considering all aspects, it does not appear to be an acceptable solution to the problem of copyright infringement. The negative impact outweighs the positive element of the action. Apart from it being unfair to impose an overly burdensome obligation to investigating all claims, it also is not effective because the content is still online. Blocking a domain name is not helping the underlying issue.

To determine whether a measure is justifiable, one has to consider proportionality as well. Blocking a domain name may be effective because the whole website is blocked so there is no access to the content, but the website may contain both lawful and unlawful material. Blocking a domain name blocks everything including all subdomains and emails so it more than likely will not be proportionate.

4.3.3 Proportionality

When assessing proportionality one has to evaluate conflicting rights at national level that enforce EU law. The fundamental rights of the EU have supremacy. So when considering a domain name block, it has to be established that blockade does not excessively interfere with the freedom to conduct business and the freedom of expression as already mentioned.

"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".[96]

[95] James Allen-Robertson, *Digital Culture Industry: A History of Digital Distribution,* Palgrave Macmillan (2013).
[96] Charter of Fundamental Rights of the European Union 2009.

This is Article 52 of the Charter concerning the scope and interpretation of rights and principles in the EU. In the Advocate General's opinion of *Telekabel*[97], it was noted that the measures ordered should not go beyond what is mandatory in reaching the objective. The cost and effort of the measure should not be excessive to the goal pursued. In the case itself, the Judge said "The Court notes that there is nothing whatsoever in the wording of Article 17(2) of the Charter to suggest that the right to intellectual property is inviolable and must for that reason be absolutely protected".[98]

There is a four step test to proportionality which was employed in the Attorney General's opinion for *Scarlet v SABAM.*[99] Firstly, it looked at the characteristics of the measure that the court had to approve, which was the filtering and blocking system, these characteristics were considered against the measure requested which was the injunction. Secondly, the measure requested were analysed in view of the directives and provisions of the Charter. Thirdly admissibility is investigated taking into account the limitations of article 52(1) of the Charter and fourthly, there has to be an examination as to whether the measure sought may be adopted on the basis of national law of the state. Injunctions for inhibiting future infringement is far more difficult because it is harder to prove proportionality when asking for so much.

4.4 Chapter Conclusion

Registrars have to a duty to act only when they become aware of the illegal content. In *L'Óreal v eBay*[100], the Court held that in order to be protected by the E-Commerce Directive, the operator must not have an active role, so it cannot have knowledge or control of the data stored. There has been increasing pressure on domain name registrars to suspend domain names, the

[97] Opinion of Advocate General of *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH.*
[98] *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH* [2014] CJEU C-314/12, par. 61.
[99] Opinion of Advocate General of *Scarlet Extended SA v Belgian Society of Authors, Composers, and Publishers SCRL (SABAM).*
[100] *L'Oréal SA and Others v eBay International AG and* Others [2011] CJEU C-324/09.

United States Trade Representatives said domain name registrars are “playing a role in supporting counterfeiting and piracy online”, and “these entities reportedly refuse to abide by the [ICANN] rules that are designed to foster legitimate activity on the internet, and instead help to create an atmosphere of lawlessness that adversely affects others”.[101]

From EU legislation and case law, we can see there is no clear guidelines for deciding the rules to prevent infringements or determining the responsibility of the registrar. It is up to the National Courts of the Member States to resolve on a case by case basis. To avoid responsibility, the registrar should be taking all reasonable steps that are expected from him. The liability of the registrar should be exceptional and limited.

EU law provides for injunctions against registrars, but it should be done as a last resort because of their fruitless nature. This is due to the fact that the legislation is unclear and if it is to become a more prominent source of redress then more formal legislation needs to be enacted to deal with the scenarios. It is likely that the *KeySystems*[102] ruling will pave the way for similar decisions by the courts in the future, where the Court held that the domain name registrar had a duty to investigate after notification of unlawful activity and had to take corrective action in the case of an obvious violation. Blocking a domain name is disproportionate and ineffective compared to other options for blocking access to content. IIS, the organisation which manages Sweden’s .se domain, stated in relation to the transfer or block order they received from the Swedish government for the domain names ‘thepiratebay.se’ and ‘priatebay.se’, “We are a quick fix but the wrong solution”.[103] ISS took a stance that they would not block these domain names because of the legal principle. They believed that domain names do not infringe copyright

[101] ‘William New, 'Annual USTR Notorious Markets Report Points Fingers, Includes Domain Registrars for First Time' (*Intellectual Property Watch*, 2015) <http://www.ip-watch.org/2015/03/06/annual-ustr-notorious-markets-report-points-fingers-includes-domain-registrars-for-first-time/> accessed 22 June 2016.

[102] *Universal Music v Key-Systems GmbH* [2014] Regional Court of Saarbrücken.

[103] 'Swedish Prosecutors Ask Court For Right To Seize Pirate Bay Domains' (*Domain & SEO News*, 2013) <http://www.domainnews.com/swedish-prosecutors-ask-court-for-right-to-seize-pirate-bay-domains/> accessed 22 June 2016

themselves. The prevalence of the online world today is due to domain names. Legislators around the world want to tackle online fraudulent activity online, but it should be done in a way that does not hamper the structure of the internet. The most fitting method for blocking access to illegal content is certainly not removing the DNS entries but it is still somewhat effective if necessary as it is cheap and quick to do. It is being used as another option at an attempt of blame for the infringement when what is required is a more adequate legal framework.

A more adequate legal framework would consist of official legislation for a notice and take down regime under Article 14 of the E-Commerce Directive. The extent of the substantiation of the notification should be made clear and it should be noted that the notice should come from a legal authority with formal knowledge who has the expertise to judge unlawful content accurately. This would provide legal certainty and harmonisation throughout the member states in an area that is currently so convoluted. It would give registrars a limited duty to respond to legal authorities. Consequently, registrars could remove a domain name upon notification and not have the burden of investigating a claim which will protect their freedom to conduct business. A more effective copyright infringement solution would be to go straight to the source and request that the website owner remove the material. The unlawful content will be remove while the lawful content will remain online. Targeting the website owner may be more cost effective than filtering as there is not long term running expenses. Filtering requires complex software that may also filter the wrong content. An adequate legal framework would also contain information for redress in case of wrongful takedown as this will contribute to the protection of the freedom of expression. The action must be done on the principle of transparency. UNESCO recommend that the laws regulating internet intermediaries should conform with international human rights including the right to

freedom of expression and should abide by the principles of accountability, transparency and due process.[104]

[104] United Nations Educational, Scientific and Cultural Organization, 'Fostering Freedom Online: The Role of Internet Intermediaries' (2016) p. 13 <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf> accessed 2 August 2016.

Chapter 5 – Thesis Conclusion

The Domain Name System has revolutionised the internet and has helped us to easily access content since its emergence. It is a valuable element to the infrastructure of the internet and it should not be exploited by society. This thesis looked at what responsibilities should be placed upon a domain name registrar, in their role as an internet intermediary, when considering illegal content on a website. It examined European legislation in this area that deals with copyright infringement and investigated fundamental rights and principles of EU law which need to be weighed up before any action should be taken. The thesis analysed under what conditions a domain name registrar is obliged to act when there is the issue of fraudulent activity on a website.

Removing a domain name as a measure to deal with illegal activity is not adequate as the content will still be available online and accessible through the IP address. A website owner may set up a link directly to an IP address so as to not use the DNS or purchase numerous other domain names that direct the user to the same IP address. In order to always be online, The Pirate Bay registered various domain names.[105] The Centre for Democracy and Technology note that seizing domain names is "ineffective yet carry significant risk of collateral damage".[106] When balanced against the right to conduct business, we can see that imposing an obligation on a registrar to investigate all claims of infringement prior to take down would severely impede on their right to entrepreneurship and innovation. It would be a strain on their resources as a block requires thorough analysis to avoid impinging on the public's right to freedom of expression. Restricting access to lawful information would amount an interference with this fundamental right. A domain name block is not proportionately effective to the goal pursued. While no measure is completely effective, a proposal that is aimed more precisely to the fraudulent content would be

[105] Known as 'hydra' domain names.

[106] Centre for Democracy and Technology, 'The Perils of Using the Domain Name System to Address Unlawful Internet Content' (2011) p. 1 <https://www.cdt.org/files/pdfs/Perils-DNS-blocking.pdf> accessed 1 August 2016.

more adequate than a domain name block because it blocks access to all content on a website, including subdomains and email addresses associated with the website.

It is impossible for domain name registrars to respond to all notifications of copyright infringement because each claim involves proving a violation of law. Registrars do not have the resources and legal expertise to determine such claims. Each case requires careful consideration as an incorrect decision to block a website impedes the freedom of expression. It is more appropriate for registrars to just respond to court orders as then the registrar can act swiftly to remove the domain name upon notification as it would be substantiated by a judicial authority. In *The Pirate Bay*[107] case in Sweden, the Court found that although the .se registry may have known of the copyright infringement, it believed the registry should still be free from liability because it is not the responsibility of the registrar to assess what content on a website is permitted. The Court agreed with the registry that they have a public function as a registrar and should only act upon a court order. The domain name was seized from the registrant but the registrar was not liable. Such an intrusion of the freedom of expression should be determined by a judicial authority. A court order can be applied for from the Member State where the registrar is based as it would be the court with jurisdiction to issue an injunction under the Enforcement Directive and the InfoSoc Directive. These directives do not conflict with the E-Commerce Directive so courts can issue injunctions when necessary. Article 3 of the Enforcement Directive states that measures, procedures and remedies shall be "effective, proportionate and dissuasive".[108] Therefore the website should have to contain a large percentage of illicit content before an injunction can be issued, as in *Twentieth Century Fox Film & Others v BT*[109] where the judge said that the infringement was on such an immense scale that it was suitable to block the whole website.

[107] *The Pirate Bay* case (B 13301-06) [2009] Stockholm District Court.
[108] Article 3 (2) of Directive 2004/48/EC.
[109] *Twentieth Century Fox Film & Others v British Telecommunications PLC* [2012] 1 All ER 806.

Under EU law, the registrar, as an internet intermediary, is obliged to block the domain name after gaining knowledge of illegal activity.[110] This knowledge should be substantiated where it has already been proven there is a copyright violation as this protects the registrar's freedom to conduct business. Not requiring registrars to invest resources into a quasi-legal analysis, which might return an inaccurate evaluation of the infringement, protects a person's right to freedom of expression. A fundamental right that has been cited as necessary in a democratic society.[111] Article 14 (1) (b) of the E-Commerce Directive states that once the service provider obtains actual knowledge then they must remove the illegal content. Article 14 also states that the registrar has to expeditiously remove the unlawful content upon obtaining this knowledge. If a duty to examine and determine cases of infringement 'expeditiously' is placed on the registrar they may decide to remove the domain name without having legal certainty as to whether the content was illicit. Erring on the side of caution to avoid costly liability for potential infringement means that the registrar may be stopping access to lawful information and this restriction on access to information is one of the primary issues with domain name blocking. It is the main argument as to why domain name blocking is not an effective solution to copyright infringement. If registrars accept all claims of infringement to be true without review then it will be taken advantage of by those who want to censor content online. This demand for a duty of care could turn into an active role thus removing the registrar from the liability limitations of the E-Commerce Directive and giving them greater control over the internet.

Registrars cannot, without prior knowledge, monitor registrations of domain names that are used for illegal practices. Nor can they seek facts demonstrating illegal activity. This is incompatible with Article 15 of the E-Commerce Directive and therefore cannot be authorised by a Member State. 'Actual knowledge' mentioned in Article 14 is not defined but it cannot not be

[110] Article 14 (1) (b) of Directive 2000/31/EC.
[111] Opinion of Advocate General of *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH,* par. 21.

interpreted as general knowledge as that would require registrars to monitor DNS entries in order to avoid liability which is not permitted. The Enforcement Directive has limitations on the implementation of IPRs and if a monitoring obligation was imposed it would clash with Article 3 of the Directive.

Registrars do not perfectly fit into the E-Commerce Directive so it can be difficult to interpret. Clarification about the legislation is undoubtedly welcome. The term 'actual knowledge' needs to be clarified for take downs under Article 14 of the Directive as this will improve harmonisation throughout the Member States, which is the purpose of the Directive. The EFF note in their submission on the consultation of the E-Commerce Directive that the Digital Millennium Copyright Act system for notice and takedown in the US has caused the removal of a large amount of lawful content.[112] Europe has to be careful not to end up with the same regime by encouraging registrars and other internet intermediaries to block access to content without due consideration. Registrars often do not have the resources or skillset to investigate every complaint, especially after the *Universal Music v Key-Systems*[113] judgement as it may open up floodgates of notifications in this area. Registrars should not have to determine legal issues and they may choose the safe option of taking down the domain name in order to retain their safe harbour under Directive 2000/31/EC. In *Universal Music v Key-Systems*[114], Universal Music brought the case when h33t.com, a torrent tracker, was sharing a copyrighted album. The registrar was liable because the court found that the copyright infringement on the website was "obvious". The court held that the registrar should have believed Universals claims after they contacted the registrants and got no reply. A self-policing role from the registrar would be more effective than governmental

[112] Gwen Hinze, 'Submission of The Electronic Frontier Foundation on the Consultation on the EU E-Commerce Directive (2000/31/EC)' (2010) P. 4
<https://www.eff.org/files/filenode/international/effeuecommercedirectiveconsultationresponse.pdf> accessed 1 August 2016.
[113] *Universal Music v Key-Systems GmbH* [2014] Regional Court of Saarbrücken.
[114] *Ibid.*

regulation because of the global span of the internet but this is not possible without a registrar exhausting their resources in such a competitive market. The level of details of the notice is the crucial factor when determining whether a domain name registrar should respond. Domain name registrars can quickly and easily remove a domain name once they are assured of the infringement, but cannot block a domain name carelessly as it has serious repercussions on a fundamental right. Restricting access to information that is both lawful and unlawful by blocking a domain name in order to protect IPRs is not proportionate. Having stricter take down requirements allows for greater protection of the freedom of expression.

"It appears that the era of blanket registrar immunity is now over, registrars would be well advised to prepare accordingly".[115]

[115] John Di Giacomo, 'New Trends in Cybersquatting law: Domain Name Registrars May Be Held Liable for Contributory Infringement' [2011] *Intellectual Property Magazine*<http://www.traverselegal.com/PDF/intellectualproperty_digiacomo.pdf> accessed 27 June 2016.

Bibliography

Books

Lehr W and Pupillo L, *Internet Policy and Economics* (Springer 2009)

Lipton J, *Rethinking Cyberlaw* (Edward Elgar Pub Ltd 2015)

Articles

Schellekens M, 'Liability of Internet Intermediaries: A Slippery Slope?' (2011) 8 SCRIPTed <http://www2.law.ed.ac.uk/ahrc/script-ed/vol8-2/schellekens.pdf> accessed 23 June 2016

Di Giacomo J, 'New Trends in Cybersquatting law: Domain Name Registrars May Be Held Liable for Contributory Infringement' [2011] *Intellectual Property Magazine*<http://www.traverselegal.com/PDF/intellectualproperty_digiacomo.pdf> accessed 27 June 2016

Saadat F and Soltanifar M, 'The Role of Internet Service Providers (ISPS) In Encouraging Customers to Use Their Internet Services in Iran' (2014) 5 International Journal of Business and Social Science <http://ijbssnet.com/journals/Vol_5_No_3_March_2014/20.pdf> accessed 28 June 2016

Cases

Association Francaise pour le Nommage Internet en Coopération Paris Court of Appeal, 19 October 2012

Belgian Society of Authors, Composers, and Publishers (SABAM) v SA Tiscali (Scarlet) [2007] District Court of Brussels No. 04/8975/A

EMI Records (Ireland) Limited, Sony Music Entertainment Ireland Limited, Universal Music Ireland Limited, Warner Music Ireland Limited and WEA International Incorporated v UPC Communications Ireland Limited (High Court Case No. 2009/5472P

Gucci America, Inc. v Hall & Associates (2001)

L'Oréal SA and Others v eBay International AG and Others [2011] CJEU C-324/09

Lockheed Martin Corp. v Network Solutions, Inc. (1997) Case No. CV 96-7438 DDP

Meyer & Partenaires v Jack Van Zandt [2007] WIPO Arbitration and Mediation Center, DFR2008-0030 (WIPO Arbitration and Mediation Center)

Productores de Música de España (Promusicae) v Telefónica de España SAU [2008] CJEU C-275/06

Universal Music v Key-Systems GmbH [2014] Regional Court of Saarbrücken

Scarlet Extended SA v Belgian Society of Authors, Composers, and Publishers SCRL (SABAM) [2011] CJEU C-70/10

The Pirate Bay case (B 13301-06) [2009] Stockholm District Court

Twentieth Century Fox Film & Others v British Telecommunications PLC [2012] 1 All ER 806

UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktion mbH [2014] CJEU C-314/12

Yildirim v Turkey [2012] European Court of Human Rights (no. 3111/10)

Ziggo BV and XS4ALL BV v BREIN, ECLI: NL: HR: 2015: 3307

Legislation

Charter of Fundamental Rights of the European Union 2009

Digital Millennium Copyright Act 1996

Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provisions of information in the field of technical standards and regulations.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000)

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001)

Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004)

European Convention on Human Rights 1953

Treaty on the Functioning of the European Union 2012

Treaty on European Union 1992

Websites

'Irish & European Website Hosting, Cloud Hosting, Exchange Hosting, Domain Registration, Dedicated Servers Ireland' (*Blacknight.com*, 2016) <https://www.blacknight.com/> accessed 23 June 2016

'Illegal Online Content And Liability Of Internet Intermediaries: Why the Messengers Should Not Be Shot' (*Diplomacy*, 2012) <http://www.diplomacy.edu/blog/illegal-online-content-and-liability-internet-intermediaries-why-messengers-should-not-be-shot> accessed 27 August 2016

'Privacy And Proxy Services | ICANN WHOIS' (*Whois.icann.org*, 2016) <https://whois.icann.org/en/privacy-and-proxy-services> accessed 23 June 2016

'Registrar Registrant Agreement' (*Blacknight.com*, 2016) <https://www.blacknight.com/registrar-registrant-agreement.html> accessed 23 June 2016

'Uniform Domain Name Dispute Resolution Policy' (*Icann.org*, 2016) <https://www.icann.org/resources/pages/udrp-rules-2015-03-11-en> accessed 23 June 2016

'New Domain Name Regulations Will Turn the Internet into the Wild West' (*OPEN Forum*, 2011) <https://www.americanexpress.com/us/small-business/openforum/articles/new-domain-name-regulations-will-turn-the-internet-into-the-wild-west/> accessed 23 June 2016

Brito J, 'Bitcoin: Imagine a Net without Intermediaries' (*Technology Liberation Front*, 2011) <https://techliberation.com/2011/04/16/bitcoin-imagine-a-net-without-intermediaries/> accessed 23 June 2016

'Wikileaks & ICE Domain Seizures Show How Private Intermediaries Get Involved In Government Censorship | Techdirt' (*Techdirt.*, 2016) <https://www.techdirt.com/articles/20101201/17390512086/wikileaks-ice-domain-seizures-show-how-private-intermediaries-get-involved-government-censorship.shtml> accessed 23 June 2016

Saez C and New W, 'WIPO Sees Decrease in Cybersquatting Complaints, Warns of Domain Name Expansion' (*Intellectual Property Watch*, 2010) <http://www.ip-

watch.org/2010/03/23/wipo-sees-decrease-in-cybersquatting-complaints-warns-of-internet-domain-expansion/> accessed 23 June 2016

'How Hollywood Plans To Seize Pirate Site Domain Names - Torrentfreak' (*TorrentFreak*, 2015) <https://torrentfreak.com/how-hollywood-plans-to-seize-pirate-site-domain-names-150120/> accessed 23 June 2016

'Bugnion - Propriété Intellectuelle - Intellectual Property' (*Bugnion.ch*, 2016) <http://www.bugnion.ch/services_internet_en.php> accessed 23 June 2016

Vallianeth T, 'Godaddy to Be Sued as an Intermediary for Copyright and Trademark Infringement' (*Spicy IP*, 2014) <http://spicyip.com/2014/04/godaddy-to-be-sued-as-an-intermediary-for-copyright-and-trademark-infringement.html> accessed 23 June 2016

'ICANN' (*Icann.org*, 2016) <https://www.icann.org> accessed 28 June 2016

Reports

Article 29 Data Protection Working Party, 'Working Document on Data Protection Issues Related to Intellectual Property Rights' (2005) <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp104_en.pdf> accessed 2 August 2016

Centre for Democracy and Technology, 'The Perils of Using the Domain Name System to Address Unlawful Internet Content' (2011) <https://cdt.org/files/pdfs/Perils-DNS-blocking.pdf> accessed 6 August 2016

Comninos A, 'The Liability of Internet Intermediaries in Nigeria, Kenya, South Africa And Uganda: An Uncertain Terrain' (2012)

<http://www.apc.org/en/system/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL.pdf> accessed 27 August 2016

Hinze G, 'Submission of The Electronic Frontier Foundation on the Consultation on the EU E-Commerce Directive (2000/31/EC)' (2010) <https://www.eff.org/files/filenode/international/effeuecommercedirectiveconsultationresponse.pdf> accessed 1 August 2016

ICANN, 'Beginners Guide to Domain Names' (2010) <https://www.icann.org/en/system/files/files/domain-names-beginners-guide-06dec10-en.pdf> accessed 23 June 2016

LegitScript and Knujon, 'Rogues and Registrars: Are Some Domain Name Registrars Safe Havens for Internet Drug Rings?' (2010) <http://www.legitscript.com/download/Rogues-and-Registrars-Report.pdf> accessed 23 June 2016

Organisation for Economic Co-operation and Development, 'The Economic and Social Role of Internet Intermediaries' (2010) <http://www.oecd.org/internet/ieconomy/44949023.pdf> accessed 23 June 2016

Organisation for Economic Co-operation and Development, 'Communiqué On Principles For Internet Policy-Making' (2011) <http://www.oecd.org/internet/innovation/48289796.pdf> accessed 7 August 2016

United Nations Educational, Scientific and Cultural Organization, 'Fostering Freedom Online: The Role of Internet Intermediaries' (2016) <http://unesdoc.unesco.org/images/0023/002311/231162e.pdf> accessed 2 August 2016

WIPO, 'The Role and Responsibility of Internet Intermediaries in the Field of Copyright And Related Rights'

<http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf> accessed 23 June 2016